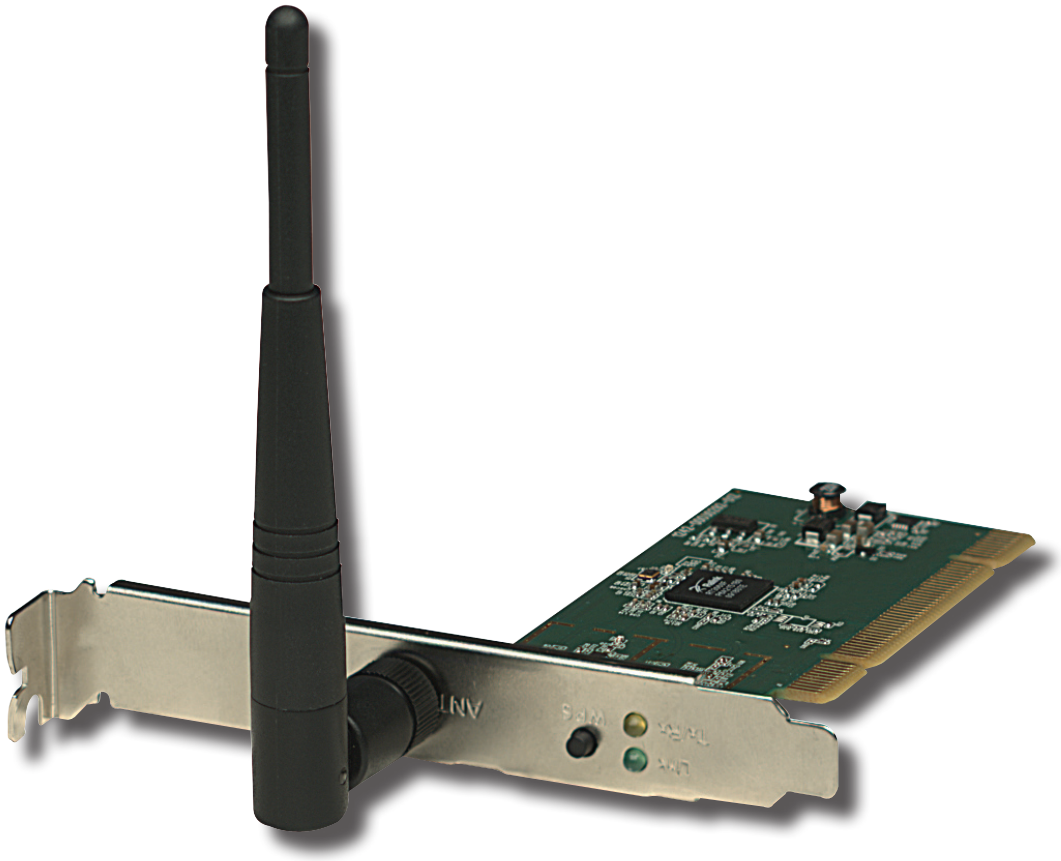
WIRELESS 150N PCI CARD USER MANUAL

MODEL 524810



INTELLINET™

NETWORK SOLUTIONS

INT-524810-UM-0110-01

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Wireless 150N PCI Card, Model 524810.

This compact high-speed adapter allows you to connect your desktop computer to wireless networks so you can transfer or receive digital images, videos and MP3 files faster than ever, connecting to the wireless network with link speeds of up to 150 Mbps using the latest in wireless technology. This adapter is also compatible with 802.11b and 802.11g wireless access points and wireless routers, giving you the flexibility to start upgrading your wireless network without the need to replace your existing equipment.

Detailed instructions in this user manual make installation reasonably quick and simple so you'll soon be enjoying the benefits of all these additonal features:

- Detachable 3 dBi antenna with reverse SMA connector
- Supports WMM (Wi-Fi Multimedia) for increased multimedia data throughput
- Supports the most popular operating systems: Windows 2000, XP, Vista and 7
- Supports Software AP function (turns your wireless client into a wireless access point)
- Tree-Year Warranty

System Requirements

- Desktop PC with Pentium 300 MHz-compatible processor or higher
- Windows 2000, XP, 2003, Vista or 7
- Available 32-bit PCI slot

Package Contents

- Wireless 150N PCI Card
- 1 antenna
- Quick install guide
- Setup CD with user manual

NOTE: Some screen images have been modified to fit the format of this manual.

SAFETY & COMPLIANCE STATEMENTS

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of Federal Communications Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or TV reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

This device and its antenna must not be co-located or operated in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation. The equipment version marketed in the U.S. is restricted to usage of the channels 1-11 only.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC of the European Parliament and the Council of March 9, 1999, on radio equipment

and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE directive repeals and replaces Directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines must therefore be followed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU Countries Not Intended for Use

None.

Safe Operating Guidelines

- The Wireless 150N PCI Card is designed for indoor use only. *Do not* expose this card to direct sunlight, rain or snow.
- *Do not* place or use this card in or near excessively hot or humid places, such as kitchens or bathrooms.
- This card can become hot when used for long time. This is normal and is not a malfunction. *Do not* place the card on paper, cloth or other flammable materials after extended use.
- There are no user-serviceable parts inside the card. If the card isn't working properly, contact your place of purchase and ask for help. *Do not* disassemble the card yourself, as doing so will void the warranty.
- If the card falls into water, *do not* use it again before it's inspected by an authorized technician, as recommended by your place of purchase.
- If strange odors or smoke emanate from the card, immediately switch the computer off and call your place of purchase for help.

TABLE OF CONTENTS

section page

1 HARDWARE 6
1.1 Card Components 6
1.2 Installing the Card 6
2 DRIVER INSTALLATION 7
3 CONFIGURATION 11
3.1 Network Settings 11
3.1.1 INTELLINET Config Utility 12
3.1.1.1 Scanning for Other Devices 12
3.1.1.2 Connecting to an AP 14
3.1.1.3 Adding an AP to Profile List 15
3.1.2 Using the WZC Utility 20
3.2 Profile Management 23
3.2.1 Add a Profile 24
3.2.2 Edit an Existing Profile 24
3.2.3 Delete an Existing Profile 24
3.2.4 Activate a Profile 24
3.3 Advanced Settings 24
3.4 View Network Statistics 26
3.5 WMM Settings 26
3.6 WPS Configuration 27
3.6.1 PBC 28
3.6.2 PIN 30
3.7 Radio On/Off 31
3.8 About 31
4 SoftAP 32
4.1 SoftAP Configuration 32
4.2 Security Settings 34
4.3 Access Control 36
4.4 Connection Table 37
4.5 Event Log 37
4.6 Statistics 38
4.7 About 39
5 TROUBLESHOOTING 40
6 FREQUENTLY ASKED QUESTIONS 41
7 SPECIFICATIONS 44

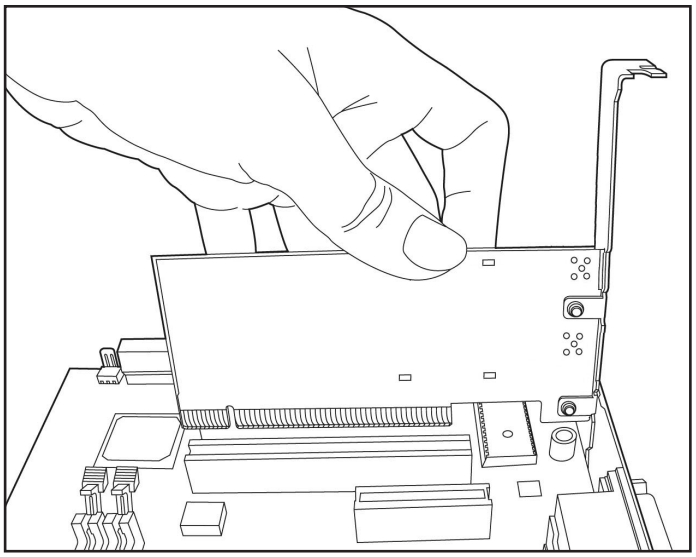
1 HARDWARE

1.1 Card Components

- Screw the included antenna onto the reverse SMA connector after the card has been installed on the computer (see below). It's recommended that the antenna be positioned at a 90˚ angle to the card initially for what is typically the best radio reception, adjusting it as needed later.
- Press and hold the WPS button for 3 seconds to start the WPS function. When WPS is enabled, the Link and Tx/Rx LEDs will light.
- The Tx/Rx LED is yellow and blinks when data is being transferred or received. When it's off, there is no wireless activity. When WPS is enabled, this LED remains on.
- The Link LED is green. It lights when a link has been established to a wireless access point; it goes off when the radio is switched off. When WPS is enabled, this LED remains on.

1.2 Installing the Card

1. Turn off the computer.
2. Remove the cover.
3. Insert the card into an empty PCI slot on the computer.
4. Attach the antenna and position it as directed above.
5. Replace the cover and turn the computer on.

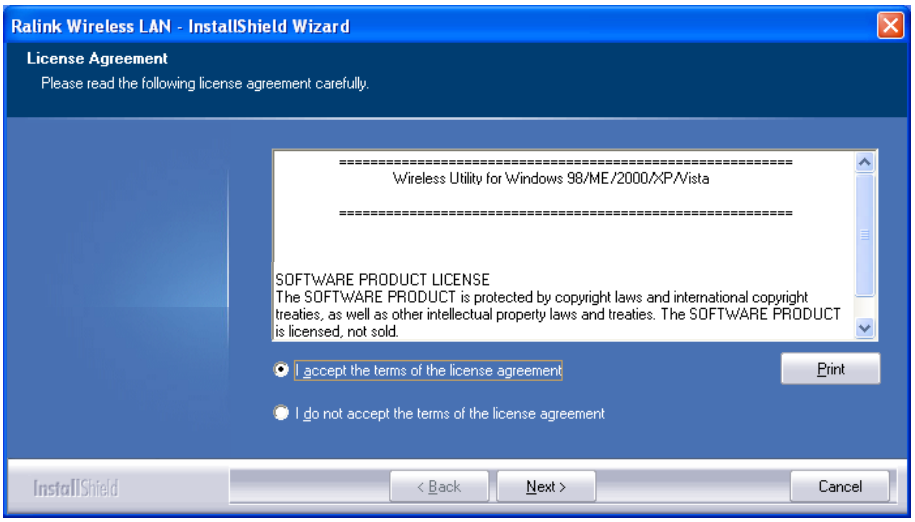


2 DRIVER INSTALLATION

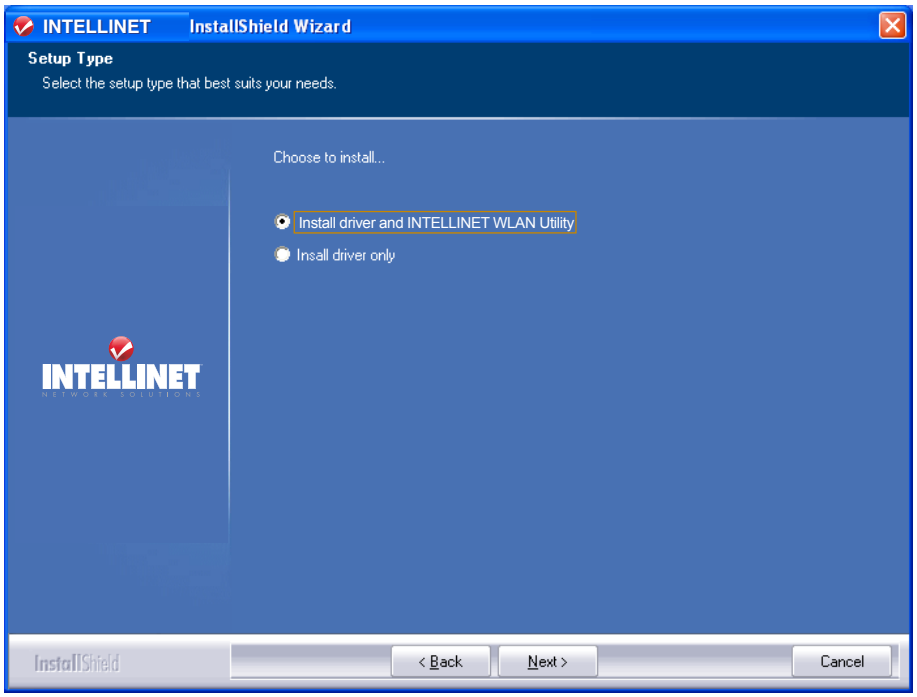
Once the Wireless 150N PCI Card is installed and the computer is turned back on, the Welcome to the Found New Hardware Wizard screen will display. Click “Cancel” and proceed with the driver installation procedure below.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

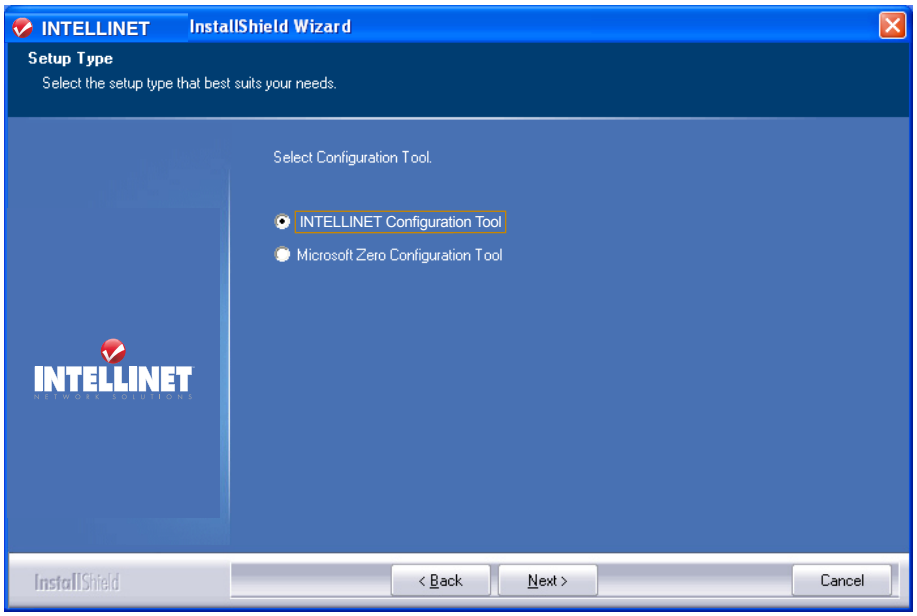
1. Insert the included setup CD and run the Setup.exe program.
2. When the License Agreement screen displays, read the agreement, select “I accept the terms of the license agreement” and click “Next.”


Ralink Wireless LAN - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
Wireless Utility for Windows 98/ME/2000/XP/Vista
SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.
I accept the terms of the license agreement
I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

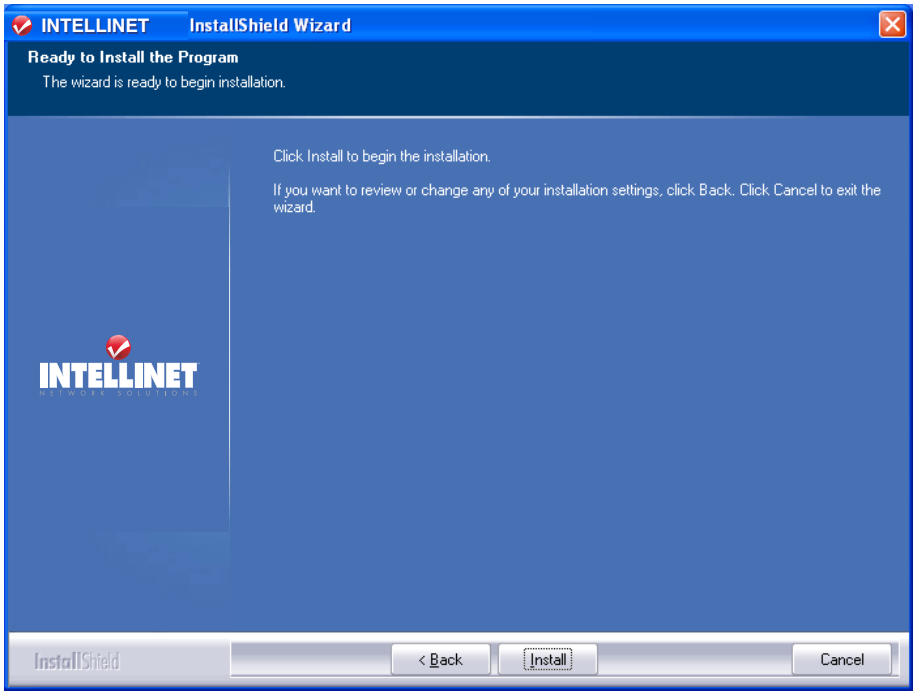
3. It's recommended that both the driver and utility be installed from the Setup Type screen if the card is being installed on this computer for the first time. Select "Install driver only" if you prefer. Click "Next"to continue.



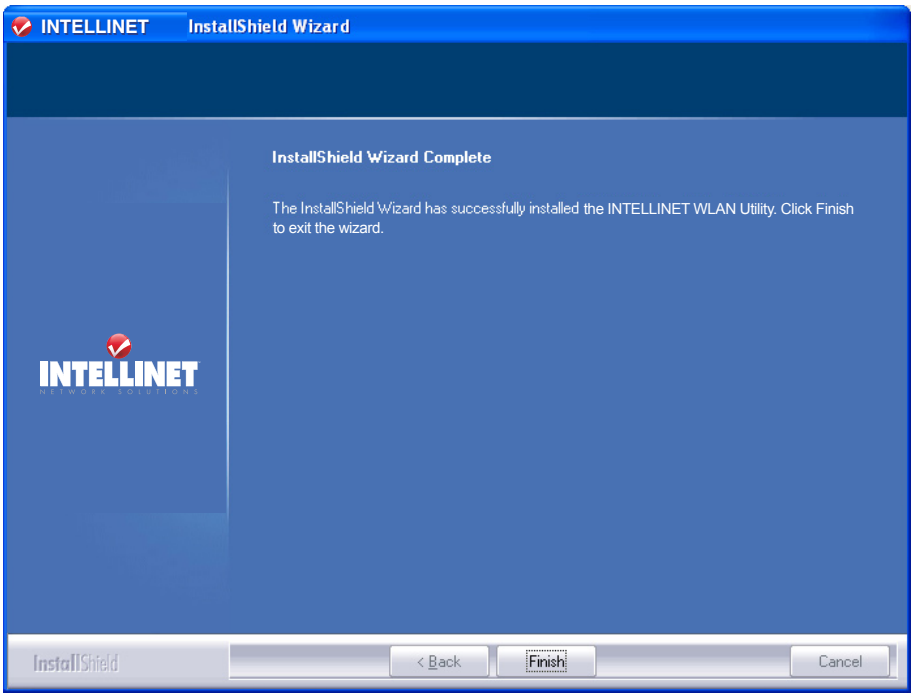
4. On the second Setup Type screen, it's recommended that you select "INTELLINET Configuration Tool," as it provides full access to all the functions of this card. If you prefer to use the wireless configuration tool provided by Windows XP or Vista, select "Microsoft Zero Configuration Tool." Click "Next."



5. When the Ready to Install the Program screen displays, click “Install.” If another Found New Hardware screen displays instead, wait a moment for the program to update, then continue. After you click “Install,” wait for the program to run.

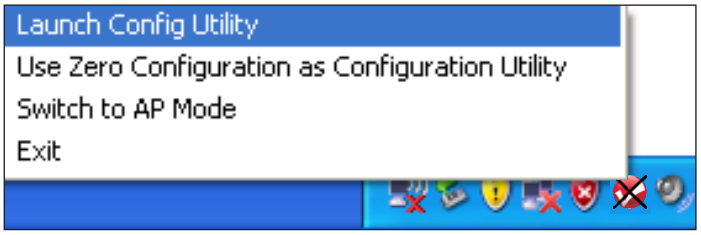

INTELLINET
InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
INTELLINET
InstallShield
< Back
Install
Cancel

6. When the final utility screen displays, click “Finish” to complete the driver installation process.



Once installation is complete, the wireless configuration utility displays on the computer desktop and as an INTELLINET icon in the systems tray. Mouse-over the icon to learn the card status.

To configure your wireless connection, right-click on the icon to display the popup menu. Click “Launch Config Utility” to start the configuration program. To close the utility, click “Exit.”



NOTE: If you click “Exit” to close the configuration utility, you won’t be able to maintain the wireless link to the access point you want to use. In this case, you can re-launch the utility by going to Start on the desktop and clicking the Wireless Utility option, as shown below.

3 CONFIGURATION

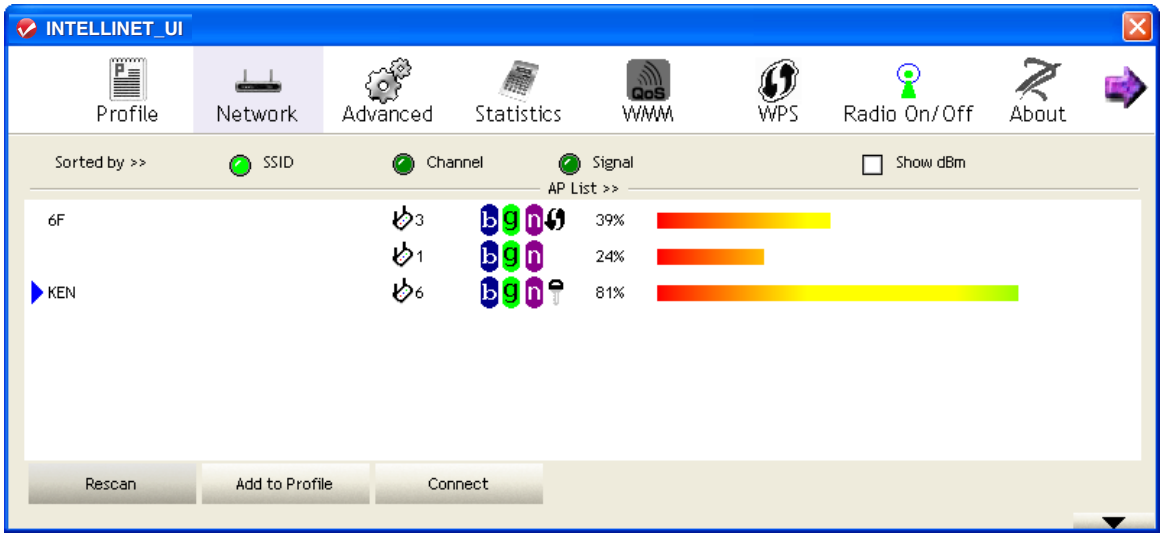
Once the driver is installed, it will automatically try to connect to any unencrypted wireless access point. If you want to connect to a specific wireless access point, or if the access point you want to connect to uses encryption, you need to configure the Wireless 150N PCI Card and input the required parameters first.

The current status of your wireless connection is indicated by the appearance of the configuration utility icon.

- The wireless connection is established: good signal reception.
- The wireless connection is established: normal signal reception.
- The wireless connection is established: weak signal reception.
- The connection is not established yet or was lost.
- The wireless network card is not detected.

3.1 Network Settings

Right-click the configuration utility icon on the desktop to display the popup menu; then click “Launch Config Utility” (as shown on Page 10). The utility will automatically begin to scan for all wireless access points and display a Network screen.



As mentioned in Section 2: Driver Installation, there are two ways to configure the card to connect to a wireless access point: using the INTELLINET configuration utility and using Windows’ built-in Microsoft Zero Configuration Tool. Both options are detailed below.

3.1.1 INTELLINET Configuration Utility

All utility screens present a menu of function options — Profile, Network, etc. — across the top. The Network screens feature a setup window below the menu section, which expands in depth automatically to accommodate information that corresponds to the current card activity. ***TIP:*** You can also expand the setup window by clicking the “More/Less” up/down arrow button at the bottom-right of the screen (clicking it again to revert back to the original window size).

3.1.1.1 Scanning for Other Wireless Devices

There are two kinds of wireless connection mode: Infrastructure and Ad-Hoc.

Infrastructure mode is used by wireless access points, which are able to establish wireless connections for you and other wireless or wired network clients.

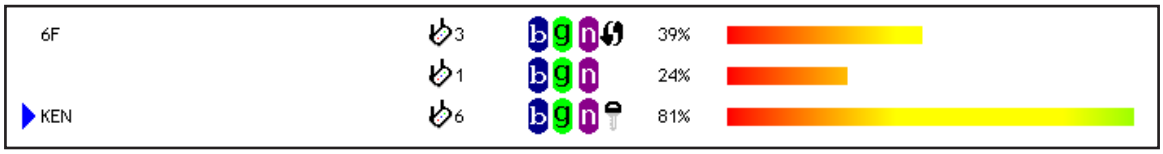
Ad-Hoc mode is also known as Point-to-Point mode. In this mode, wireless devices such as computers or PDAs will not be capable of establishing wireless connections with more than one wireless device, and so is suitable for establishing a one-to-one wireless connection between two wireless devices.

Before you can connect to any wireless access point or device by Infrastructure or Ad-Hoc mode, there two pieces of information you need to have:

- The wireless device’s SSID, or service set identifier (which you can think of as an access point’s name). You can scan for the SSID of other wireless devices nearby, but if the SSID of the wireless device you want to connect to is hidden, you need to know it — exactly — before you can establish a connection with it.
- The wireless device’s encryption key (if it uses encryption).

When the scan results are displayed in the setup window, check that the wireless device (access point or another computer) with the SSID you want to connect to is included.

Scan results include several pieces of information:



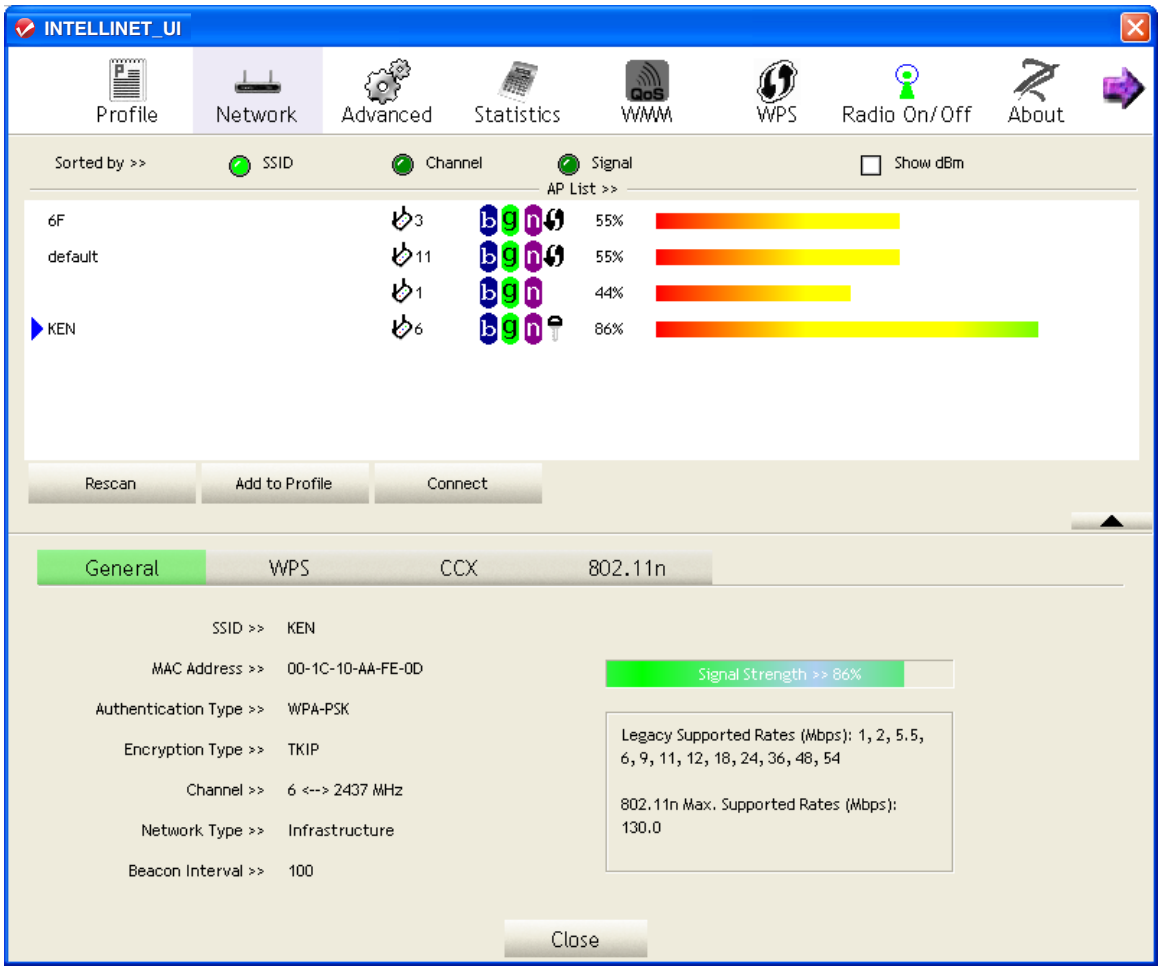
- The wireless device’s SSID is displayed to the left (KEN, 6F in the example above). If nothing appears, it means the SSID of that device is hidden. When a connection is established, a blue arrow ( ) displays to the left of the SSID.
- The type and channel number of the wireless device, depicted by if it’s an AP or by if it’s a computer (Ad-Hoc mode, point-to-point connection)
- The wireless standard supported by this access point: “n” for 802.11n; “g” for 802.11g; and “b” for 802.11b. Additionally, the WPS icon ( ) will appear when the access point supports WPS; a key icon ( ) will appear if the access point uses

encryption. ***NOTE:*** When the access point supports WPS and the WPS icon appears, you won't see the key icon here even through the access point uses encryption.

- The signal strength of the access point as a percentage (100% = full strength).
- The signal strength of the access point as a bar graph (as a visual comparison).

If you don't see the access point you want, click "Rescan" until the AP you prefer is displayed. If rescanning doesn't find the AP you want after five tries, move your computer closer to the access point or refer to Section 5: Troubleshooting.

To see detailed information about a specific access point, double-click on it. The expanded screen presents four more packets of information in addition to the options and details already displayed.



Sorted by >> — You can sort all listed access points: by SSID, channel or signal (strength).

Show dBm — Check this box to show the signal strength in decibels instead of as a percentage.

Rescan — Click to rescan for access points.

Add to Profile — To store a specific access point in the Profile List (see Section 3.1.3: Add an Access Point to Profile) so that you can link to it directly without entering the authentication key again, select the AP, then click "Add to Profile."

Connect — Click to connect to whichever access point is selected on the list.

General —Displays basic information about the selected access point, such as SSID, MAC address, authentication/encryption type, channel and such.

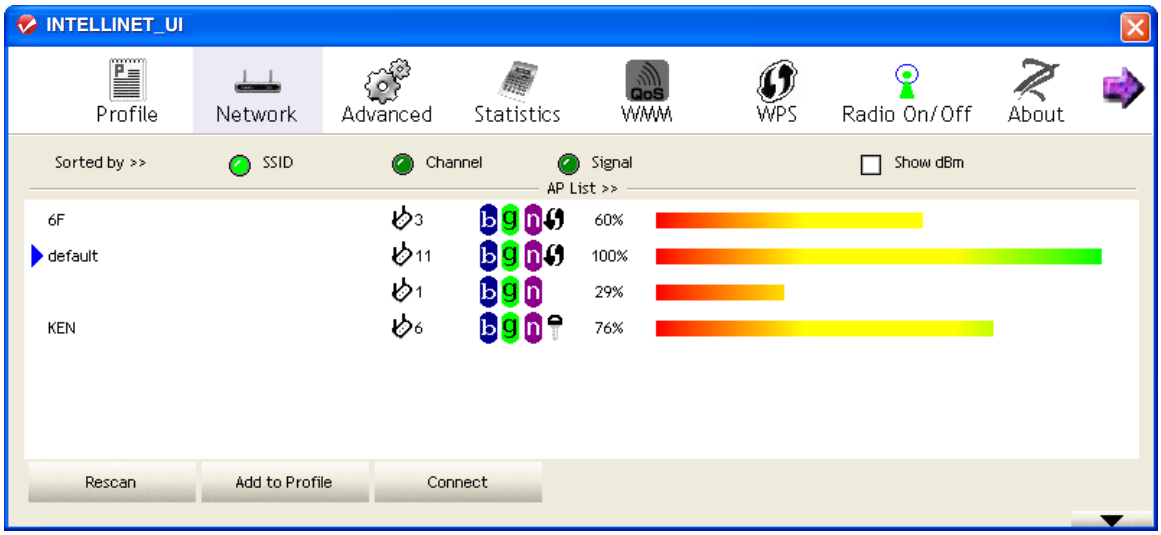
WPS — If this access point supports WPS (Wi-Fi Protected Setup), related information is displayed here.

CCX —If this access point supports CCX (Cisco Compatible eXtension), related information is displayed here.

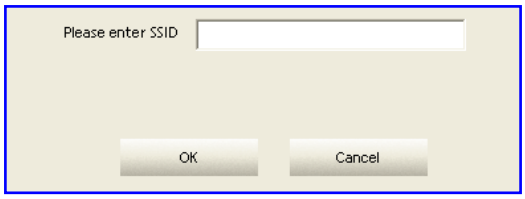
802.11n — If this access point complies with the 802.11n draft, related information is displayed here.

3.1.1.2 Connecting to an Access Point

1. Select the wireless access point or network device you want to connect to and click "Connect." If the access point you selected doesn't use encryption, you'll be connected to it within a minute. If it *does* use encryption, go to Step 3.

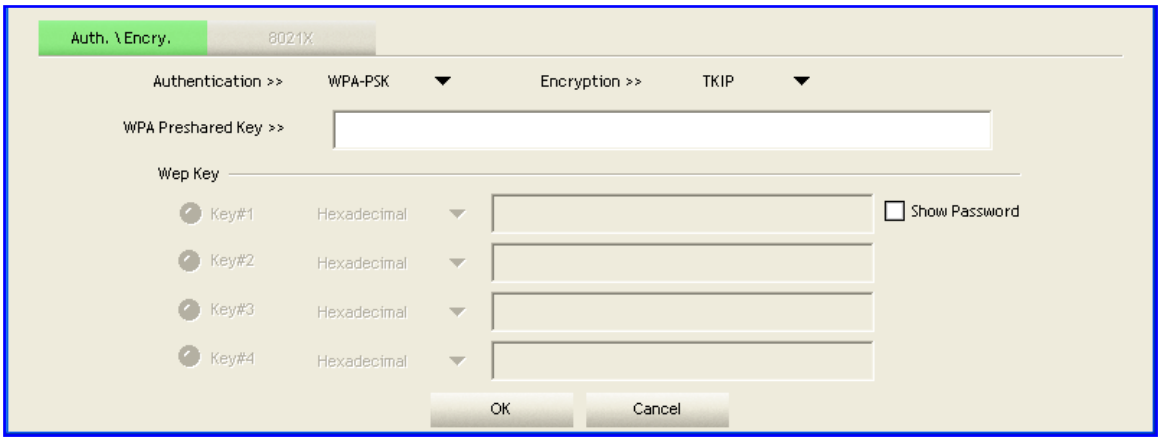


2. If the wireless access point doesn't show an SSID, you'll be prompted to enter it. ***NOTE:*** If you need to obtain the SSID from the owner of the wireless access point you're connecting to, make sure it's exact or the connection won't work. Once you've entered the SSID, click "OK."



3. If the wireless access point uses encryption, you will be prompted to enter its WEP key or WPA preshared key. ***NOTE:*** If you need to obtain the key from the owner of the device you're connecting to, make sure it's exact or the connection

won't work. Check the "Show Password" box to display the key you enter. The authentication type will be selected automatically by the access point: Don't change it. However, if you're connecting to an AP using 802.1x authentication, you need to select "802.1x" and enter the related information as explained later.

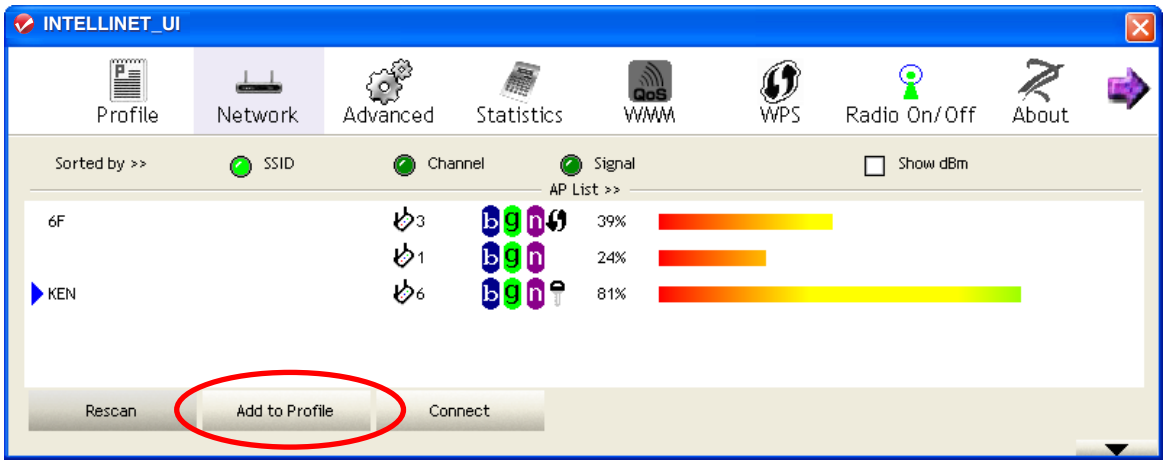


4. If the connection is successful, the blue arrow displays to the left of the SSID. Remember, you can mouse-over the configuration utility icon to display a popup that tells you the connection quality/status, and you can click the "More/Less" button ( ) to expand the screen and see more detailed information.

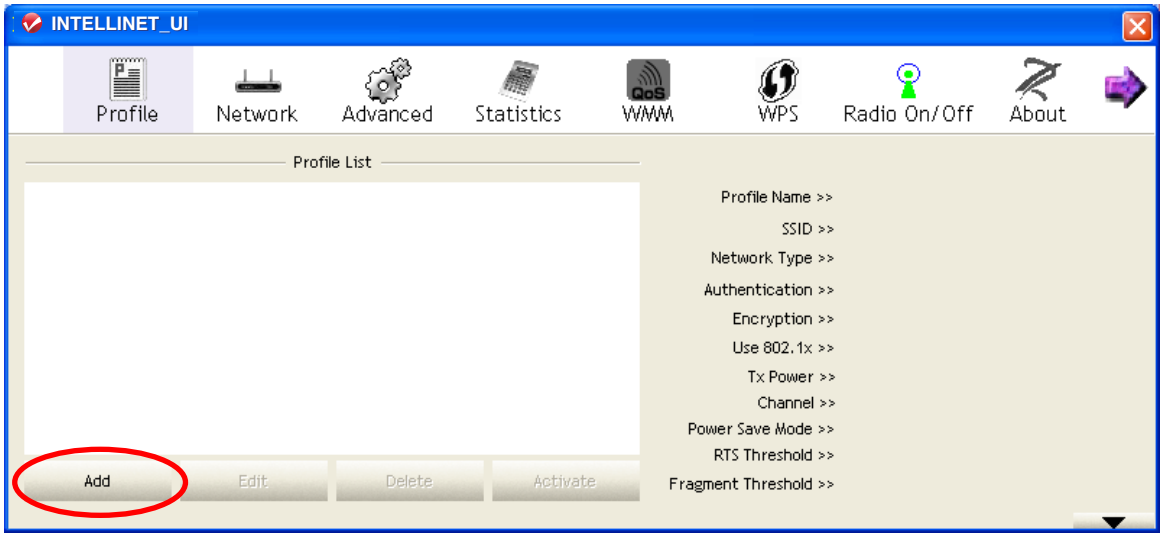
3.1.1.3 Adding an Access Point to the Profile List

If you expect to connect to a specific wireless access point frequently, you can add its information to the Profile List and recall it whenever you want to establish the connection. You can add a found access point to the Profile List, or you can enter the information of an AP manually.

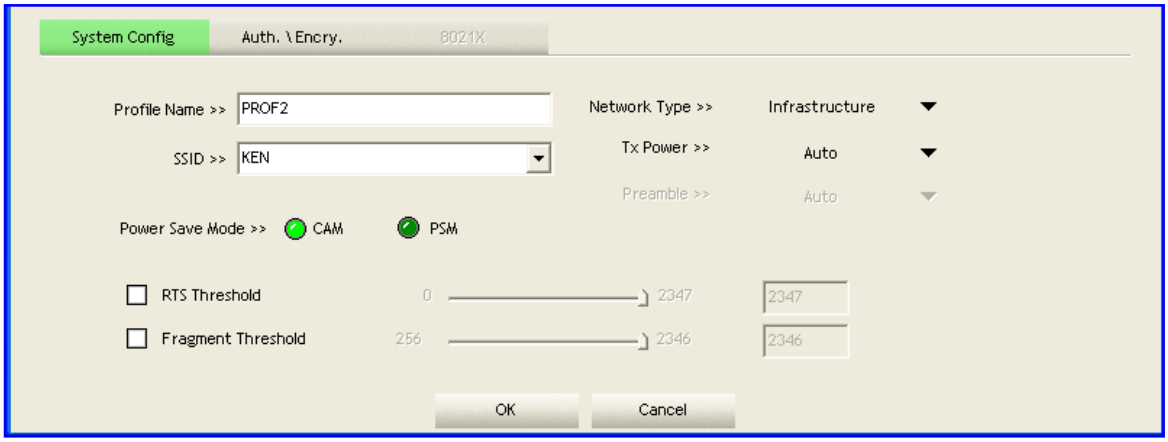
To add a found AP to the Profile List, simply select it and click "Add to Profile."



To enter the information for an access point manually, go to the Profile menu (see Section 3.2: Profile Management) and click “Add.”



The screen will expand as needed, initially displaying the System Config screen.



Profile Name — Every profile needs a unique name.

SSID — Enter the SSID of this access point. If you selected an access point from the Profile List and its SSID isn’t hidden, the SSID will be filled automatically; however, you can modify the SSID manually.

Network Type — Select Ad Hoc or Infrastructure. If you’re connecting to an access point, select “Infrastructure”; for point-to-point wireless connection (i.e., you’re connecting to another computer that’s using Ad Hoc mode), select “Ad Hoc.” ***NOTE:*** If you selected an AP from the Profile List, keep this field unchanged.

Tx Power — This is the wireless output power. If you’re not too far from an access point (good signal reception), you can select a lower output power to save energy; for a more distant access point, select a higher output power. ***NOTE:*** “Auto” is suggested to let the utility decide the best output power setting.

Preamble — Select the preamble for Ad Hoc mode here. Options are “Auto” and “Long.” Auto” is suggested to let the utility decide the optimal preamble.

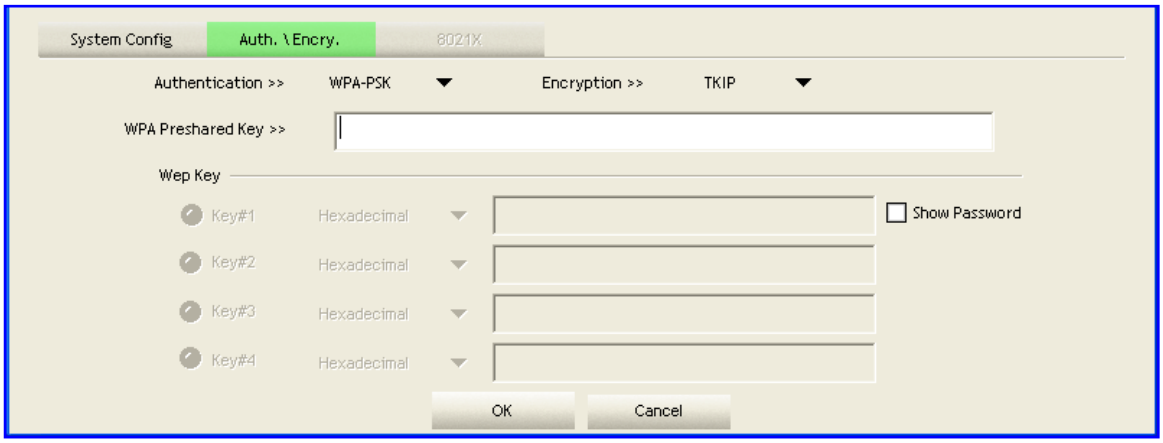
Channel — Select the radio channel for Ad Hoc mode.

Power Save Mode — Select “CAM” (Constantly Awake mode, which maintains wireless radio activity even when not transferring data), or “PSM” (Power-Saving mode, which switches the radio off when not transferring data). ***NOTE:*** PSM is recommended if you’re using this card with a notebook computer so the battery lasts longer.

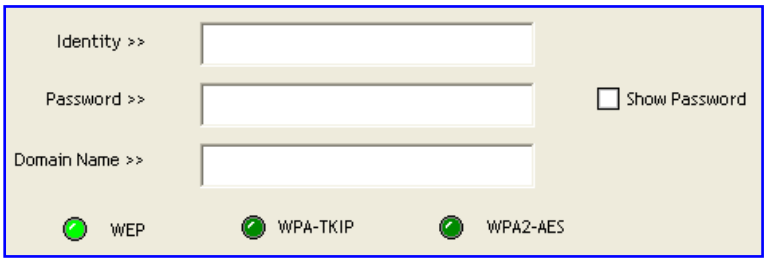
RTS Threshold — Check this box to set the RTS threshold manually, either by moving the slider to set the value, or by entering the value in the box at right. ***NOTE:*** It’s recommended that you not change this setting unless you know the effect of changing it.

Fragment Threshold — Check this box to set the packet fragment threshold manually, either by moving the slider to set the value, or by entering the value in the box at right. ***NOTE:*** It’s recommended that you not change this setting unless you know the effect of changing it.

To enter authentication/encryption information for the AP, click “Auth. \ Encry.”



Authentication — Select the authentication type of the device you want to connect to. When you’re adding a profile from an existing access point or wireless device, the authentication type will be selected automatically: Don’t change it. ***NOTE:*** If you select “LEAP,” you’ll be prompted to enter an identity, a password and a domain name, and to select an encryption type. Check “Show Password” and the password you enter will be displayed as you type it in the text field.



Encryption — Select the encryption type of the device you want to connect to. When you're adding a profile from an existing access point or wireless device, this will be selected automatically: Don't change it.

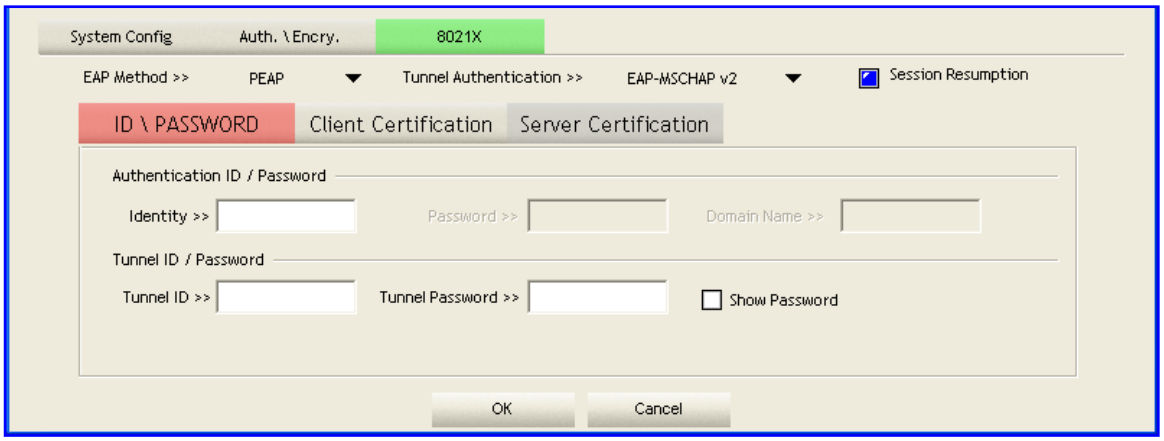
WPA Preshared Key — Enter the key here. If encryption isn't enabled, or if you select "WEP" as the encryption type, this field will be disabled and grayed out.

WEP Key — Select the key type ("Hexadecimal" or "ASCII") and input the WEP key. If encryption isn't enabled, or if you select "WEP" as the encryption type, this field will be disabled and grayed out. You can set up to four WEP keys here.

There are two types of WEP key: hexadecimal and ASCII. For a hexadecimal key, you can input numbers 0-9 and letters a-f; for example., "001122aabbcc." For an ASCII key, you can input numbers 0-9 and letters a-z; for example, "mywepkey12345." The length of a WEP key depends on the type. You can enter 10 or 26 hex characters; 5 or 13 ASCII characters.

Show Password — Check this box and all passphrases or security keys you enter will be displayed as you type.

Use 802.1x — If the AP you want to connect to requires 802.1x authentication, select "Use 802.1x," then click "802.1X" to set the 802.1x parameters.

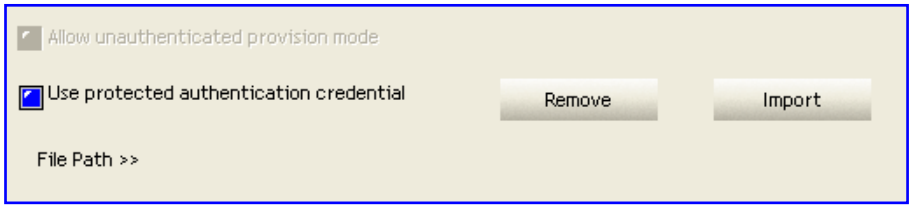


EAP Method — Select an option from the drop-down menu. ***NOTE:*** You may need to request the correct EAP method from the administrator of the AP you want to connect to.

Tunnel Authentication — Select an option from the drop-down menu. ***NOTE:*** You may need to request the correct tunnel authentication method from the administrator of the AP you want to connect to: This drop-down menu is only available when the authentication type you use is PEAP, TLS/Smart Card or TTLS.

When you use EAP-FAST as the authentication type, the protocol setting is always "Generic Token Card," which can not be changed. You also need to select "Soft Token" or "Static Password"' as the password in "ID \ Password."

The EAP Fast authentication type also displays a sub-menu for setting additional parameters specific to this option.



If you need to use protected authentication credentials, select “Use protected authentication credential” and click “Import” to load the .pac credential file. To remove a loaded credential file, click “Remove.”

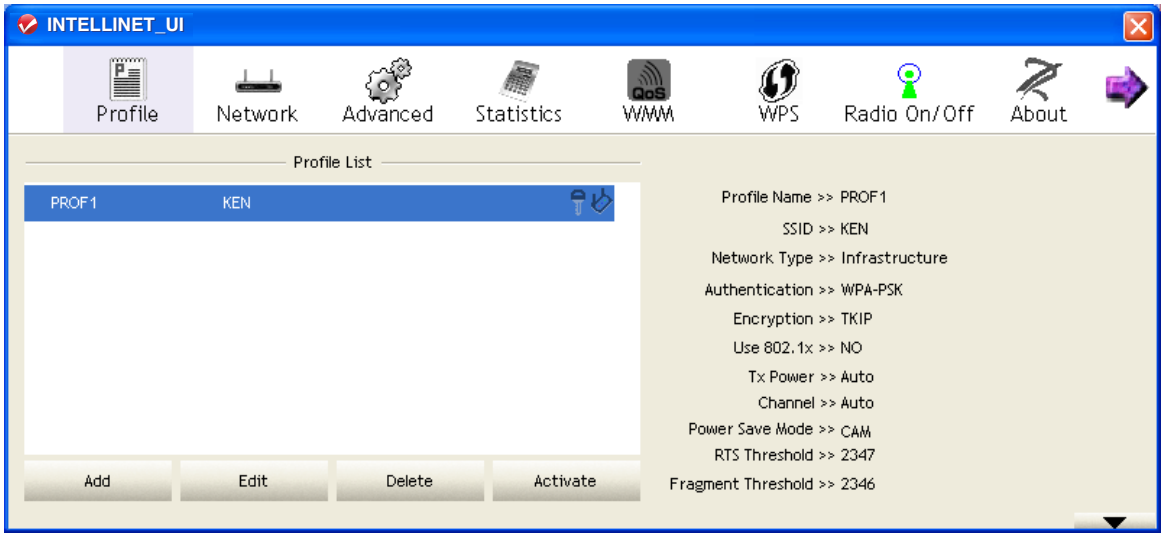
Session Resumption — Enable or disable session resumption. If you don’t know whether or not you should, ask your 802.1x authentication administrator.

ID \ Password — Input the 802.1x username (ID), password and other information (if required). Click “Show Password” to show the password you entered.

Client Certification — Click to select a local certificate from the drop-down menu. If the AP you want to connect to requires a specific client certificate, the certificate must be installed on your computer. You can select the certificate here.

Server Certification — Click to use server-based certification. Select a CA (certificate authority) from the drop-down menu. If intermediate certificates are allowed, select “Allow intermediate certificates.” Also, if you need to specify the CA server’s name, you can specify it in the “Server name” field. If you select “Server name must match,” the CA server’s name must be the same as the value you entered in the “Server name” field. If you prefer that only the domain name part of the full server name match the value you set in the “Server name” field, select “Domain name must end in specified name.”

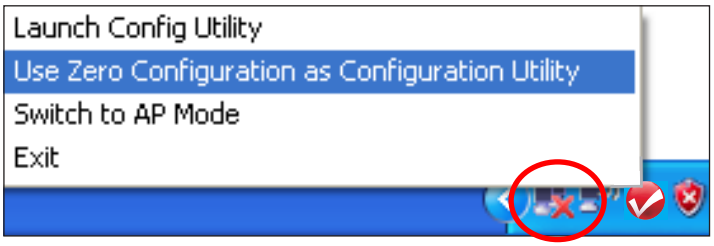
Once you’ve finished entering all the information related to the access point, click “Activate.” The profile will display in the Profile List.



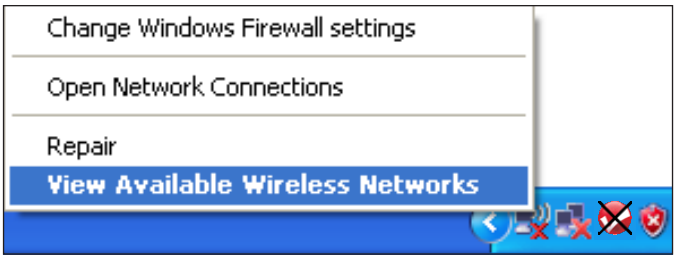
3.1.2 Using the Windows Zero Configuration Utility

Windows XP, Vista and 7 have a built-in wireless network configuration utility called Windows Zero Configuration (WZC), which you can use as an option for configuring your wireless network parameters.

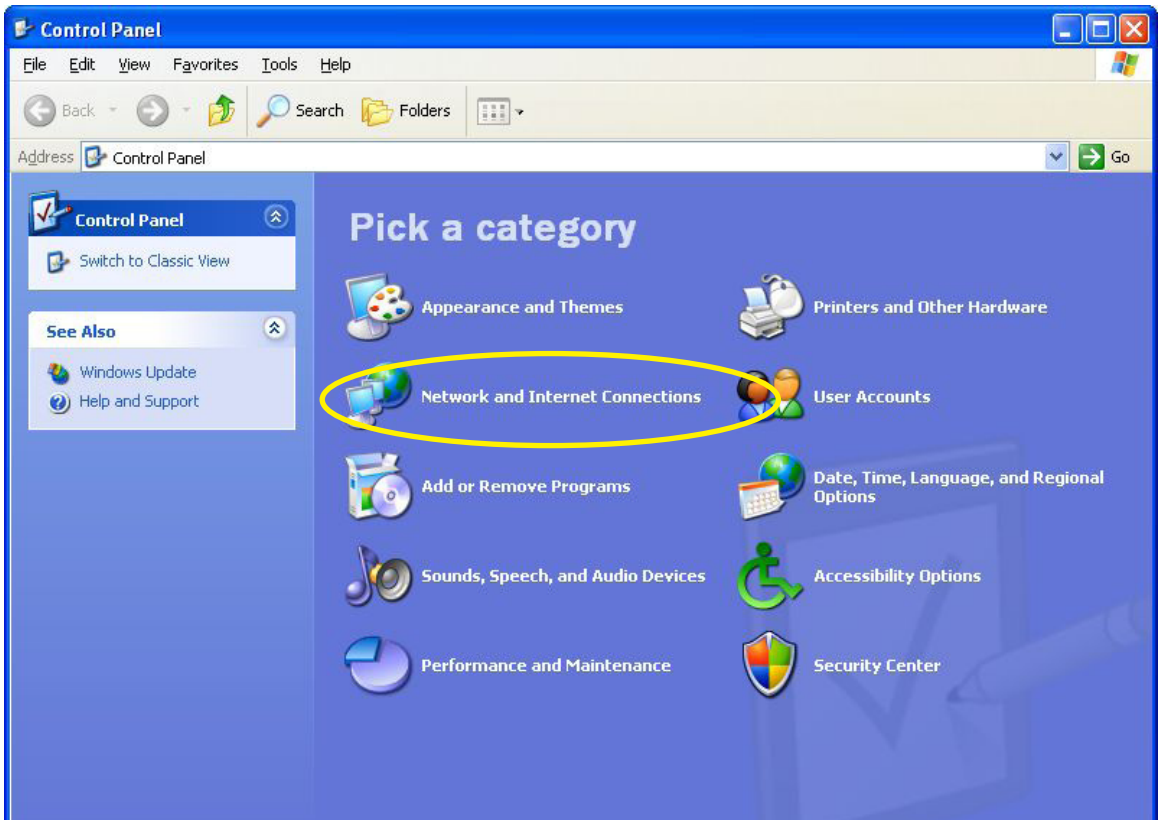
1. Right-click the INTELLINET configuration utility icon and select “Use Zero Configuration as Configuration utility.”



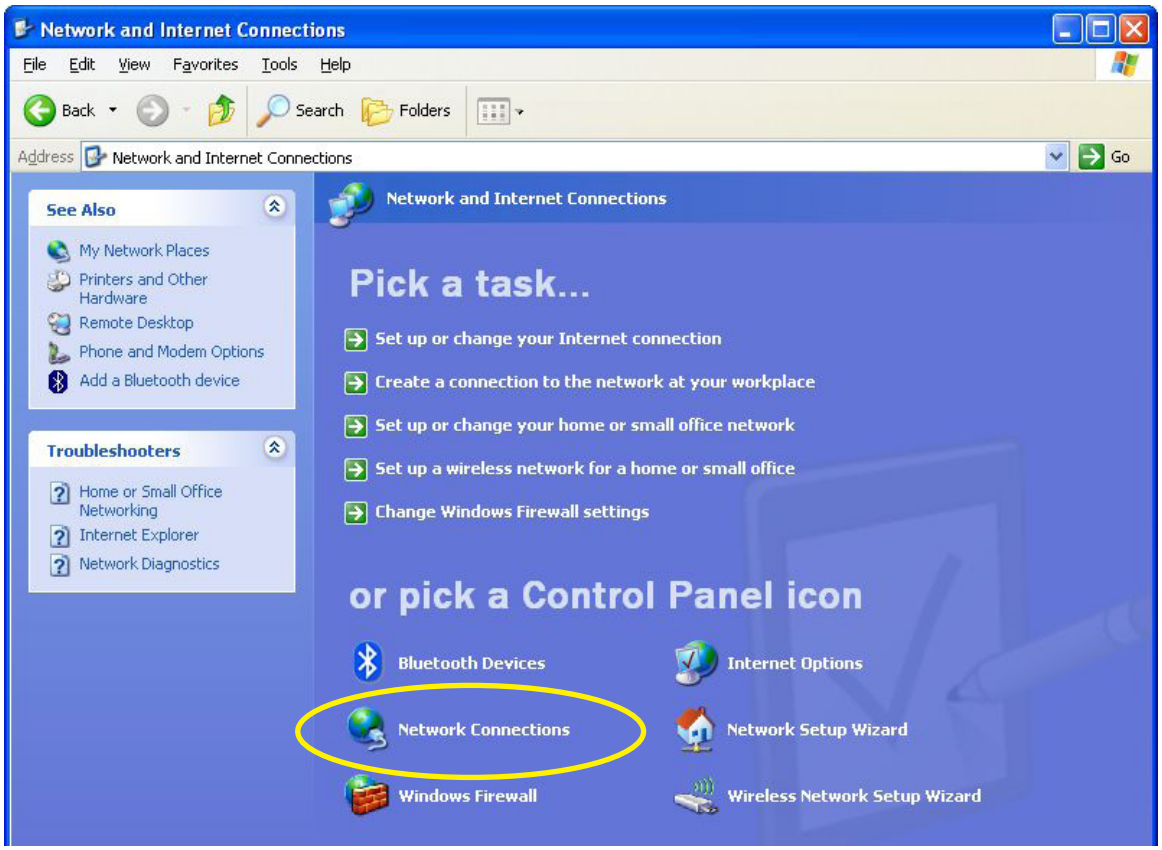
2. Right-click the Windows Zero Configuration icon and select “View Available Wireless Networks.” If you can’t find the icon, follow Steps 3 through 5 below.



3. Click “Start” on your desktop, then click “Control Panel,” then click “Network and Internet Connections.”

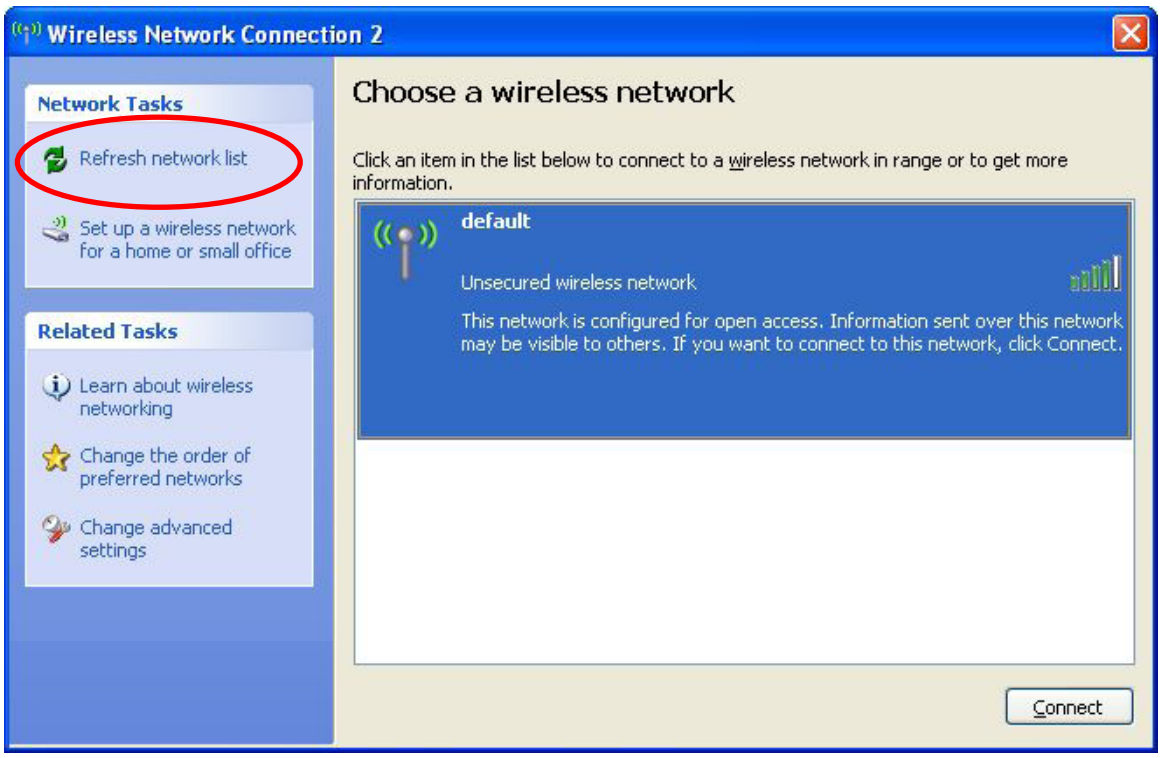


4. Click “Network Connections.”

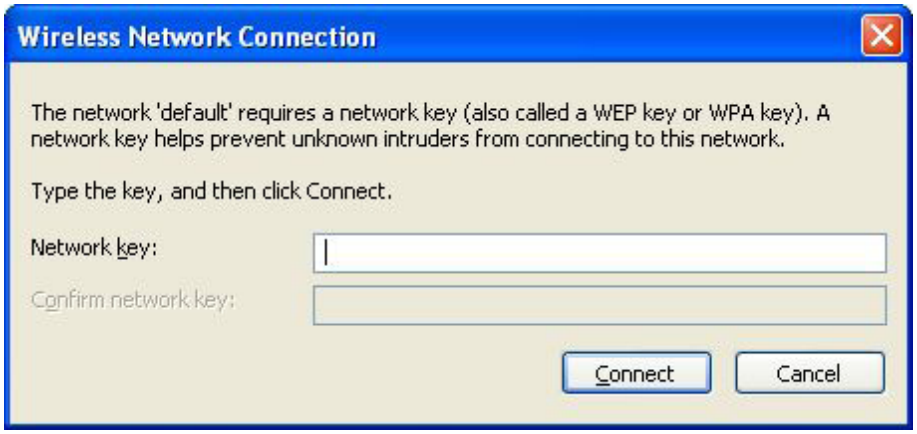

Network and Internet Connections
File Edit View Favorites Tools Help
Back Search Folders
Address Network and Internet Connections
Go
See Also
My Network Places
Printers and Other Hardware
Remote Desktop
Phone and Modem Options
Add a Bluetooth device
Troubleshooters
Home or Small Office Networking
Internet Explorer
Network Diagnostics
Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Bluetooth Devices
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

5. Right-click “Wireless Network Connection” (it may have a number as a suffix if you have more than one wireless network card, so be sure to select this Wireless 150N PCI Card), then select “View Available Wireless Networks.”

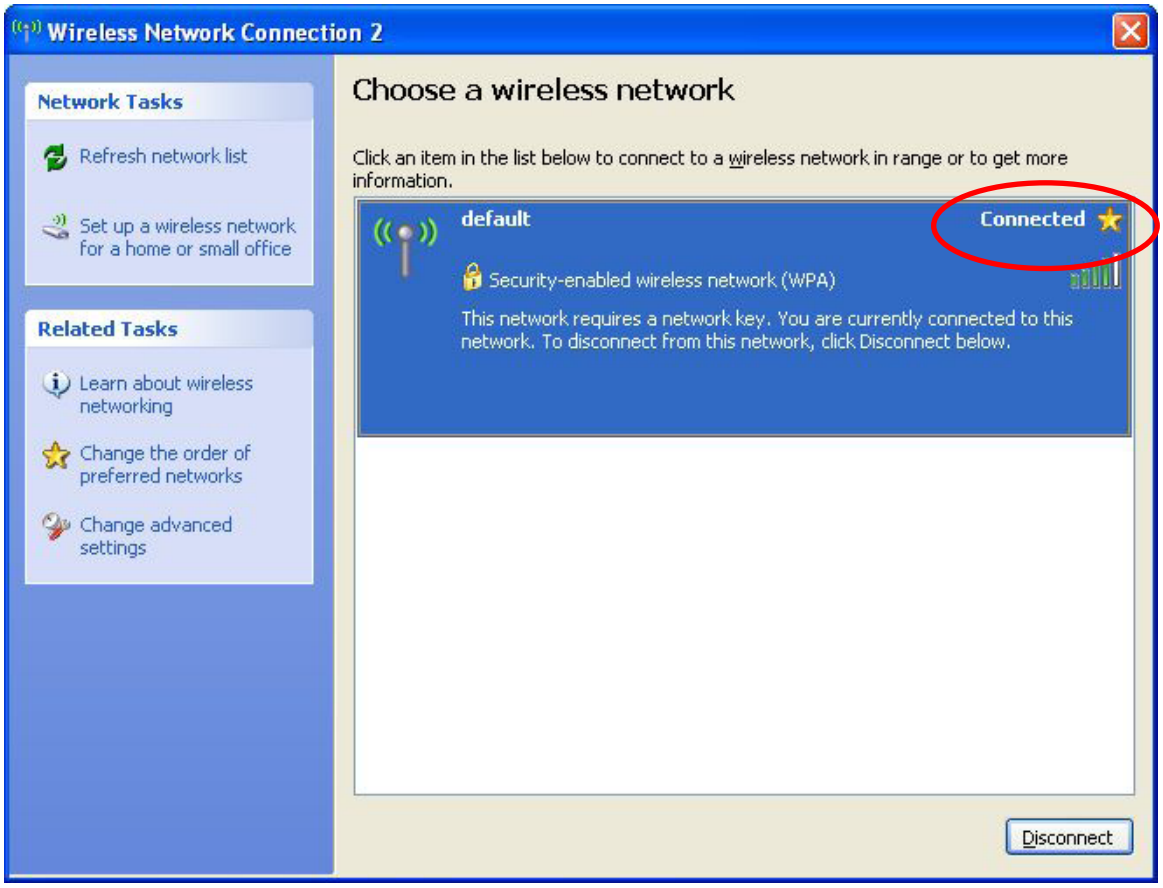
6. All wireless access points in proximity will be displayed. If the access point you want to use isn't shown, try moving your computer closer to the AP, or click "Refresh network list" to rescan access points. Select the access point you want to use if it's shown, then click "Connect."


Wireless Network Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
default
Unsecured wireless network
This network is configured for open access. Information sent over this network may be visible to others. If you want to connect to this network, click Connect.
Connect

7. If the access point is protected by encryption, you need to input its security key or passphrase here, then click "Connect." Remember, the key you enter must match the encryption setting on the access point. ***NOTE:*** If the access point you selected doesn't use encryption, you won't see this prompt.

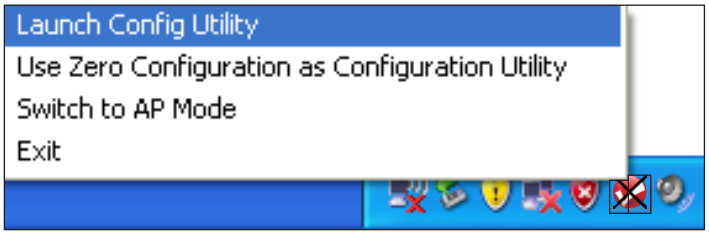

Wireless Network Connection
The network 'default' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Type the key, and then click Connect.
Network key:
Confirm network key:
Connect
Cancel

8. If "Connected" displays, the connection between your computer and wireless access point has been successfully established.

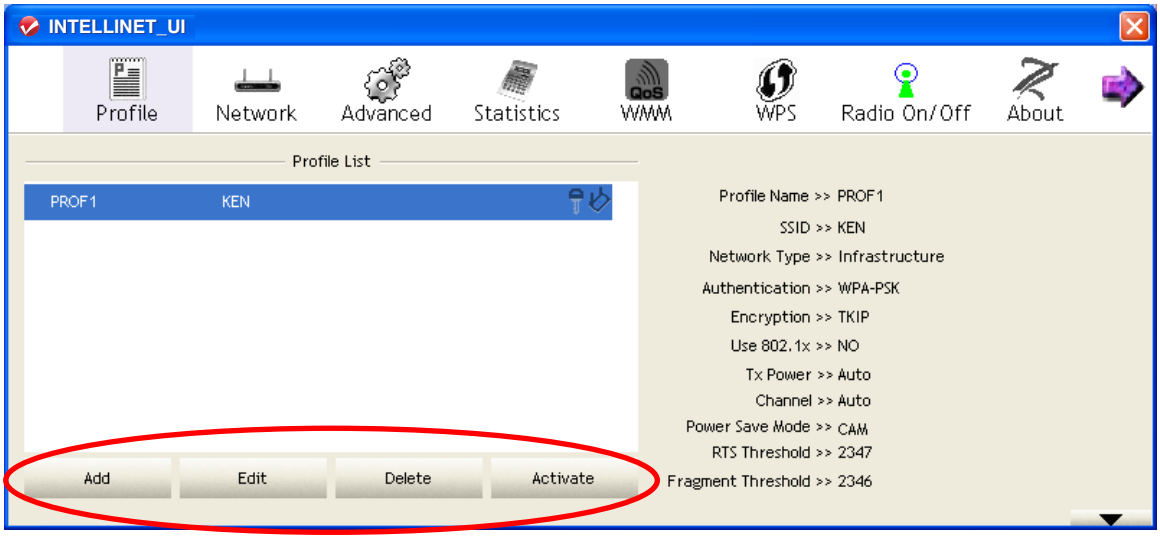

Wireless Network Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
default
Connected
Security-enabled wireless network (WPA)
This network requires a network key. You are currently connected to this network. To disconnect from this network, click Disconnect below.
Disconnect

3.2 Profile Management

If you need to connect to different wireless APs at different times — such as when you're at a cybercafe or using a public wireless service — you can store the connection parameters (encryption, security, passphrase, etc.) as a profile for every access point so you don't have to keep entering the parameters every time you want to connect to a specific wireless AP. To manage profiles, right-click the configuration utility icon and click "Launch Config Utility."



Click the "Profile" menu. All profiles will be displayed in the Profile List (as shown in the image below), and when you select a profile from the list, all information about it will be shown.



3.2.1 Add a Profile

To add a new profile, go to the Profile screen, then click “Add” (as shown above). Enter details about the access point, as described previously in Section 3.1.1.3.

3.2.2 Edit an Existing Profile

If you’ve added a profile before and want to change its contents, select it in the Profile List and click “Edit” (as shown above). The profile’s settings will display for you to modify. Click “OK” to save changes, or click “Cancel” to discard changes.

3.2.3 Delete an Existing Profile

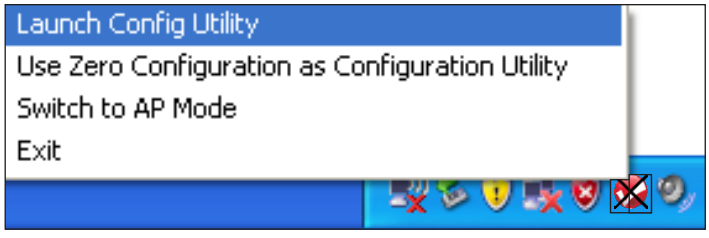
If you no longer need a profile, you can delete it simply by selecting it in the Profile List and clicking “Delete” (as shown above).

3.2.4 Activate a Profile

To connect to a specific wireless device in the Profile List, select it and click “Activate” (as shown above). When you click to activate a selected profile and a gray arrow (▶) displays in front of the profile, it means that the connection attempt failed. When the connection is successfully established, a blue arrow (▶) will be displayed.

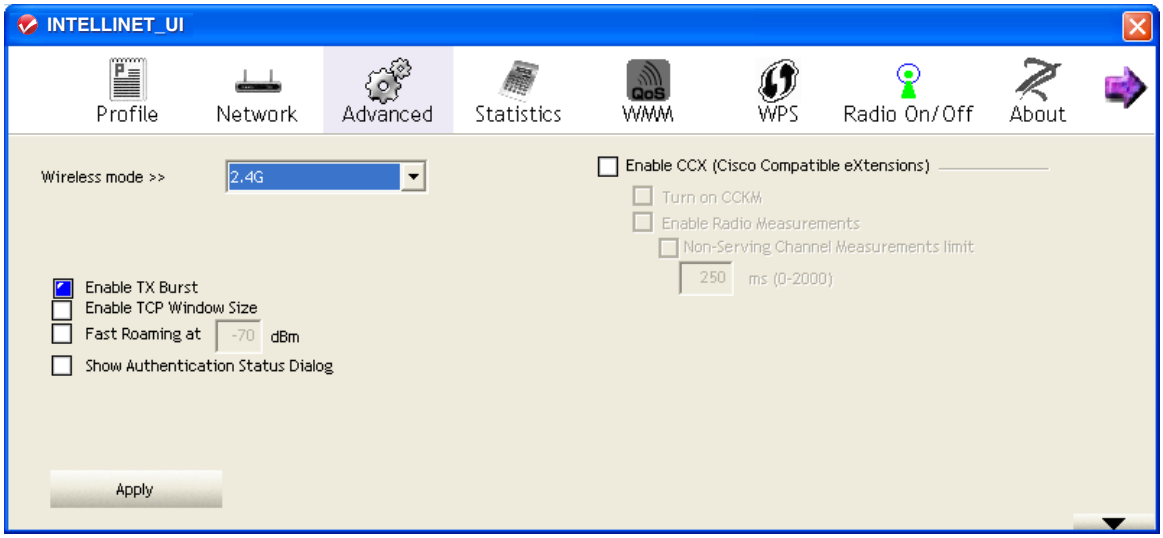
3.3 Advanced Settings

The card provides several advanced settings so experienced wireless users can change operation modes or increase data transfer performance.



1. Right-click the configuration utility icon and click “Launch Config Utility.”

2. Click “Advanced” to display the Advanced Settings screen.



Wireless mode — Click to display the wireless operation mode of the card.

Enable Tx Burst — Check this box to accelerate the data transmit rate. ***NOTE:*** It may not work with all wireless access points and wireless devices.

Enable TCP Window Size — Check this box and the configuration utility will adjust the TCP window size automatically to improve performance. ***NOTE:*** This should be safe for most wireless environments, but if you notice any data transfer problem or irregularity, uncheck this option.

Fast Roaming — Check this box to control the threshold at which the card should switch to another wireless access point with better signal quality. ***NOTE:*** Only adjust value if you understand what it means and you need to roam among multiple access points.

Show Authentication Status Dialog — When your computer is being authenticated by a wireless authentication server, a dialog window showing the authentication process will display. This function can help find the problem when you can’t be authenticated, so you can then provide this information to the authentication server’s administrator for debugging purposes.

Enable CCX — Enable Cisco Compatible eXtensions is a wireless feature developed by Cisco to improve the wireless performance with CCX-compatible wireless devices. When you check this box to connect to CCX-compatible wireless devices, the following setup items will become available.

- Turn on CCKM: Check this box to enable CCKM (Cisco Centralized Key Management), which enables wireless clients to roam among CCKM-enabled access points in a very short amount of time.
- Enable Radio Measurements: When you’re connecting to a CCX-compatible access point, check this box to enable the radio measurement function in order to improve wireless connectivity.

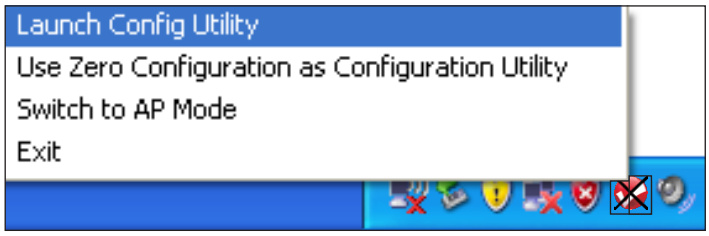
- Non-Serving Channel Measurements Limit: When you're connecting to a CCX-compatible access point, check this box to enable measurements of unused radio channels in order to improve wireless connectivity.

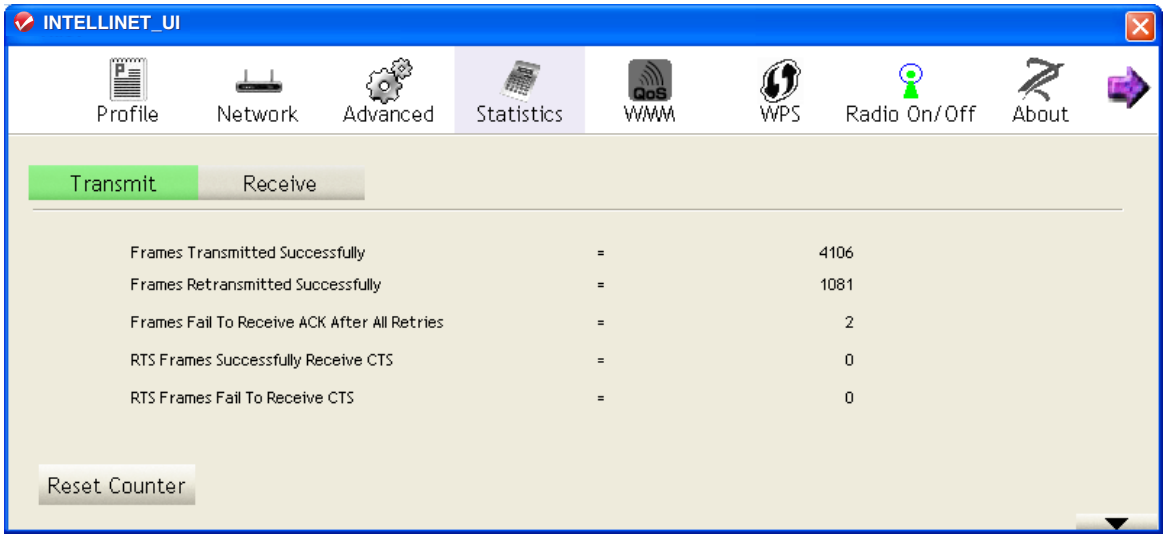
After you finish the settings, click "Apply" so they take effect.

3.4 View Network Statistics

The configuration utility provides information about network statistics and link status. To see how your wireless network card is working, you can use these functions to get detailed information about the wireless connection you're using.

1. Right-click the configuration utility icon and click "Launch Config Utility."
2. Click "Statistics" to display the screen and connection-related statistics.



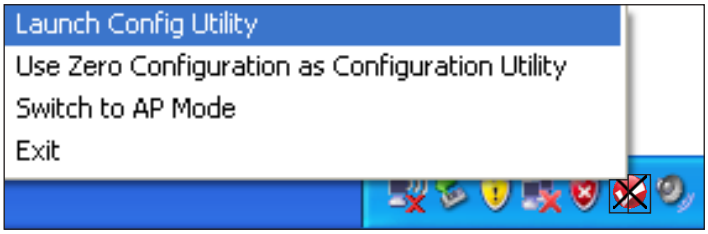


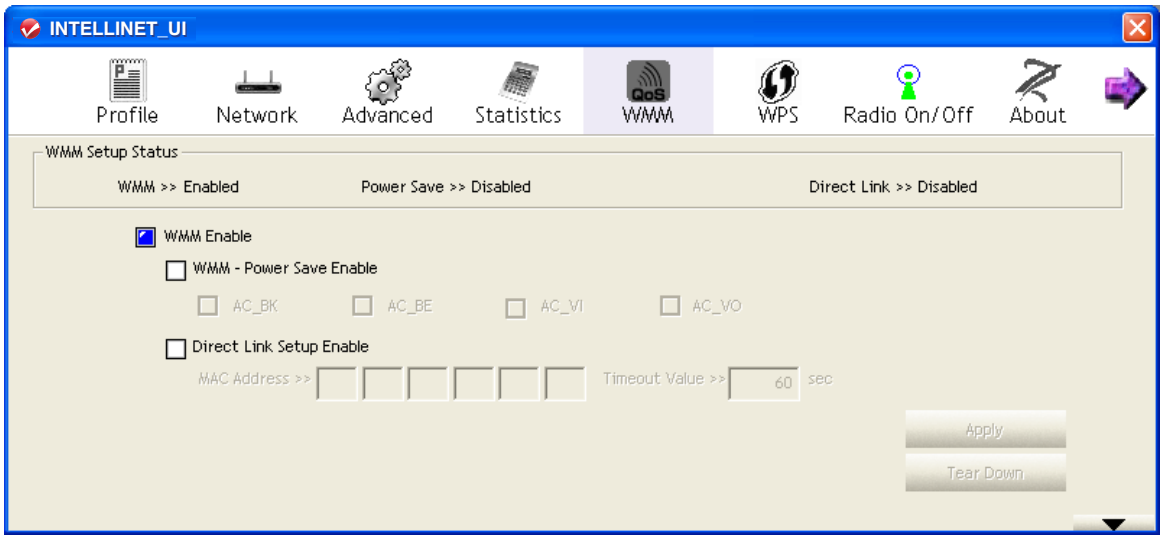
Transmit/Receive — Click either to view the corresponding statistics of any packets.
Reset Counter — Click to reset the statistics of all items back to 0 (zero).

3.5 WMM Settings

This Wireless 150N PCI Card features a WMM (Wi-Fi Multimedia) function, which can improve the performance of certain network applications, like audio/video streaming and network telephony (VoIP). When you enable the WMM function, you can define the priority of different kinds of data to give higher priority to applications that require instant response, thus improving the performance of such network applications.

1. Right-click the configuration utility icon and click “Launch Config Utility.”
2. Click “WMM” to display the screen. ***NOTE:*** In the WMM Setup Status panel, the current WMM settings are displayed.





WMM Enable — Check this box to enable the function. Click “Apply” after you check or uncheck this box so corresponding settings in this window will be activated or deactivated.

WMM–Power Save Enable — When you check this box to save energy, you also need to select one of the four modes:

- AC_BE: best performance
- AC_BK: worst performance
- AC_VI: video data has priority
- AC_VO: voice data has priority

Direct Link Setup Enable — If you have another WMM-enabled wireless device, you can enter its MAC address here. Click “Apply” and this card will establish a direct link to the wireless device you’ve specified. ***NOTE:*** You also need to specify the timeout value of this directly linked wireless device. Valid values are from 1 to 65535 (seconds). Enter “0” (zero) for infinity. To remove a specific wireless device from the direct link table, select the device and de-select this option to remove it.

3.6 WPS Configuration

Wi-Fi Protected Setup (WPS) is wireless network technology that makes wireless

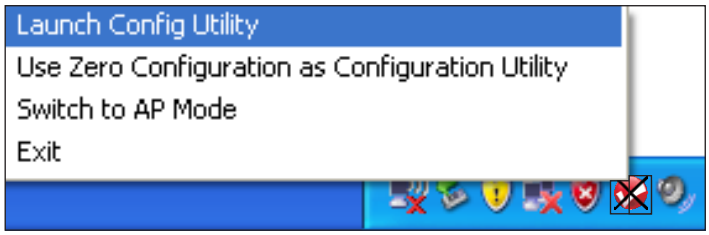
network setup relatively simple. If you have a WPS-enabled wireless access point and you want to establish a secure connection to it, you don't need to configure the device and set up data encryption by yourself: All you need to do is go to the WPS setup screen, click an on-screen option, and press a specific button or enter an 8-digit code on the wireless AP you want to establish a secure connection with — just three simple steps!

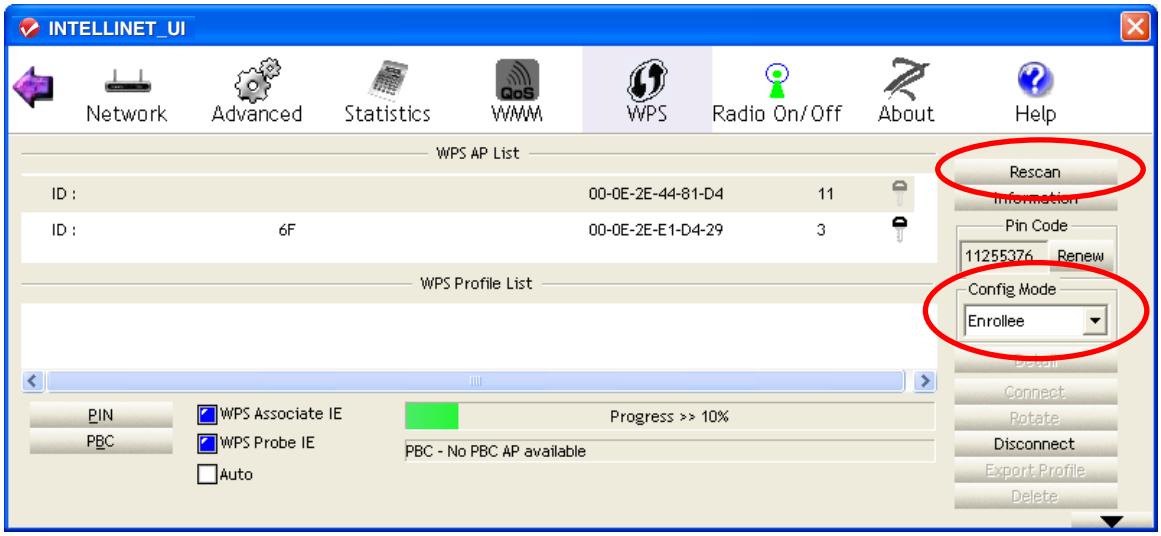
For older wireless access points, it's even possible to perform a firmware upgrade to create a WPS-enabled access point. Since older devices may not have a button to press for WPS setup, you can use an alternative WPS setup method: entering the PIN code. Every WPS-compatible wireless network card supports the PIN code configuration method: You just enter the code and the wireless access point and wireless card will do the rest for you.

Though this Wireless 150N PCI Card is compatible with WPS, the wireless access point you want to connect to must support WPS, too. Once you've confirmed that it does, proceed with the steps below.

3.6.1 WPS Setup: PBC (Push-Button Configuration)

1. Right-click the configuration utility icon and click "Launch Config Utility."
2. Click "WPS" to display the screen.





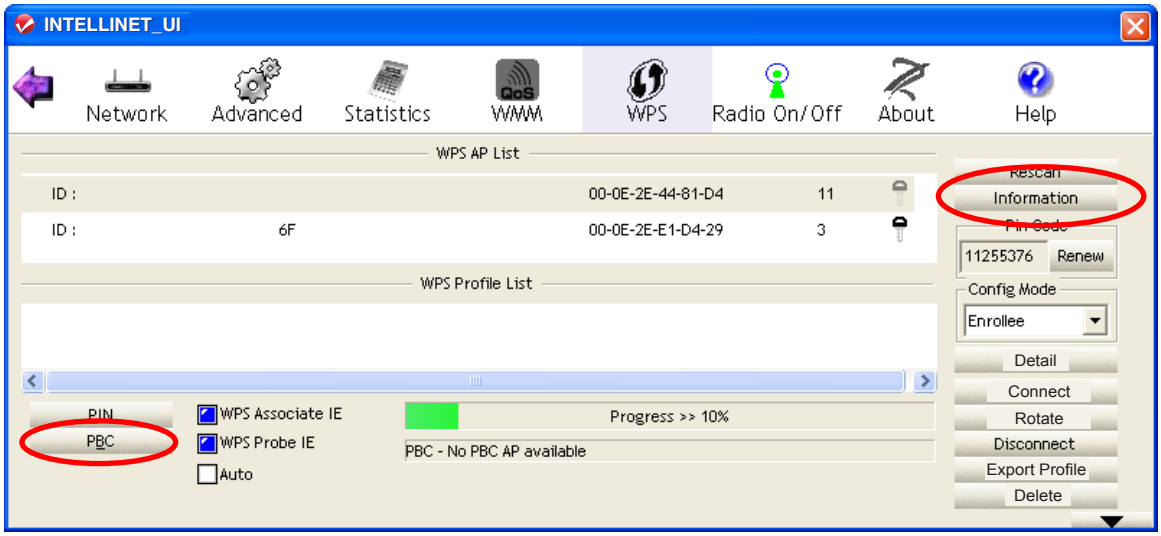
3. Set "Config Mode" to "Enrollee," then press the WPS button on your wireless AP (the button used to activate WPS standby mode may have another name).
   NOTE: Refer to the device's user manual for any other procedure/process.

You can also set “Config Mode” to “Registrar.” In this mode, this card will wait for other WPS-enabled access points to send WPS pairing requests. Again, refer to each device’s user manual to understand how to send WPS requests.

4. Before you begin to establish the wireless connection by using WPS, you can click “Rescan” to search for WPS-enabled access points near you again in order to ensure the WPS function of your access point is activated.

   All access points with WPS function enabled will be displayed in the WPS AP List window. Check that the access point you want to connect to is displayed. If it isn’t, click “Rescan” few more times. You can also click “Information” to see detailed information about the selected access point.

5. Start the PBC pairing procedure on the access point side (refering, as needed, to the instructions provided by your access point’s manufacturer), then click “PBC” on the utility screen (below) to begin establishing the wireless connection by WPS. ***NOTE:*** This may require a minute or so to complete. When you see the ‘WPS status is connected successfully’ message beneath the Progress field, the connection between this card and the access point is okay, and information about access point you’ve connected to will be displayed.



Detail — Click to see details about the connected device.

Export Profile — Click to save this connection as a profile.

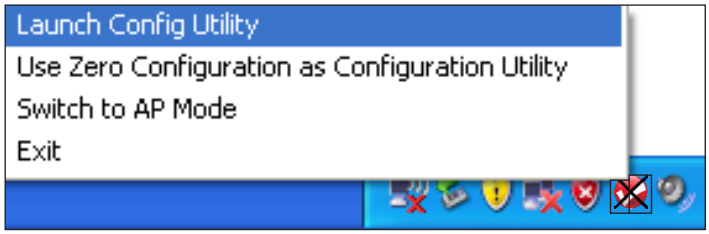
PBC — On occasions when WPS pairing fails (as shown on the screen above — “No PBC AP available” — because no WPS-enabled access point is found) you can click “PBC” a few more times to try again. When an access point is connected, you can click “Disconnect” and continue establishing connections to other WPS-enabled APs that may be found.

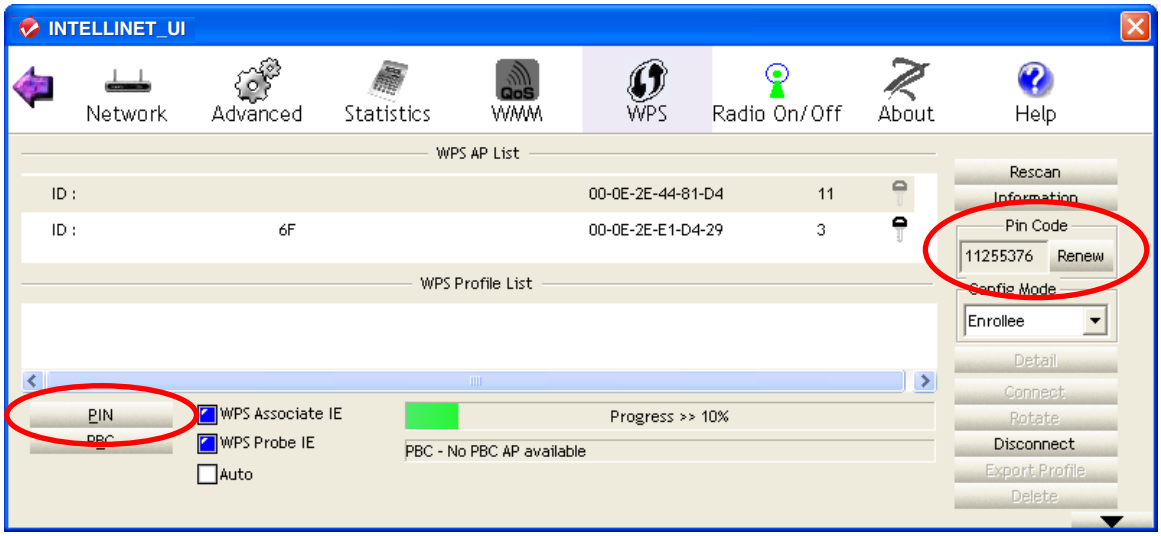
Rotate — Click to highlight the next access point on the list.

Delete — Click to remove a device from the WPS AP List.

3.6.2 WPS Setup: PIN

1. Right-click the configuration utility icon and click “Launch Config Utility.”
2. Click “WPS” to display the screen.





3. The PIN code of your Wireless 150N PCI Card is an 8-digit number located at the upper-right of the configuration utility. Make a note of it, and enter it in the “WPS PIN Code” field. (Refer as needed to the user manual of your wireless access point for instructions as to how to do this.) **NOTE:** If you experience a problem with the PIN code provided, you can click “Renew” to obtain a new PIN code.
4. Click “PIN” and wait for a few seconds to one minute. If a wireless access point with the correct PIN code is found, you’ll be connected to it. You may need to click “PIN” a few times. If you still can’t connect this way, check that the PIN code you provided to the access point is correct.

WPS Associate IE — Check this box to send the association request with WPS IE during WPS setup. This is optional: You can use the default value if you don’t know what will be affected.

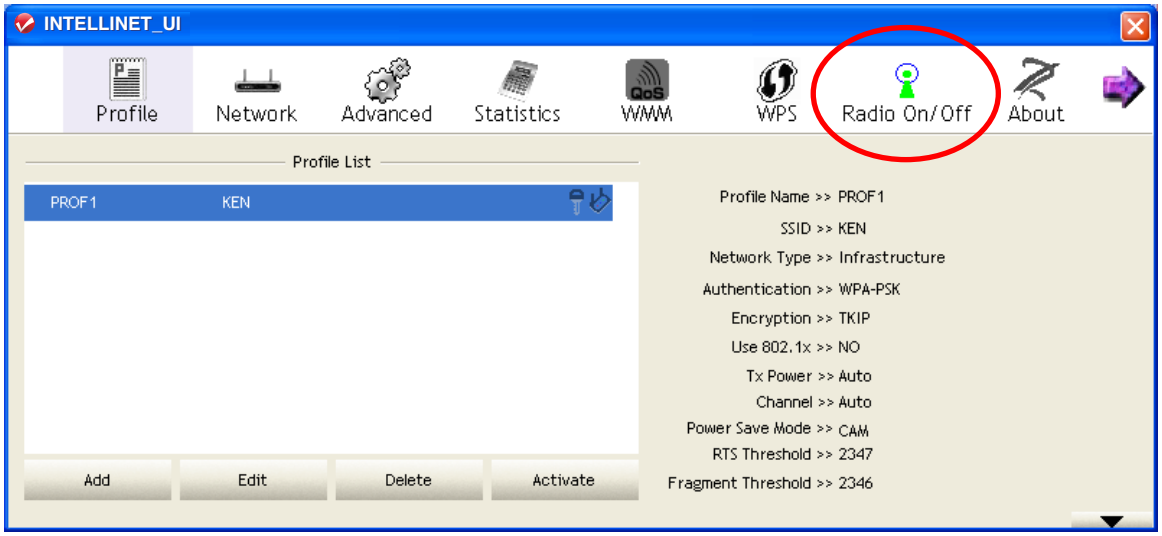
WPS Probe IE — Check this box to send the WPS probe request with WPS IE during WPS setup. This is optional: You can use the default value if you don’t know what will be affected.

Auto — Check this box in PIN mode and the wireless access point to be connected to will be selected automatically.

3.7 Radio On/Off

You can switch the wireless radio transceiver on and off by using the utility, so you don't need to physically remove the card to disable the wireless network function.

1. From whichever section you're currently viewing in the utility, you'll see the Radio On/Off icon in the menu bar of the screen. Otherwise, right-click the configuration utility icon and click "Launch Config Utility."
2. To switch the wireless radio on/off, simply click "Radio On/Off." When the icon is green (as shown below), the radio is on; when it's red, the radio is off.

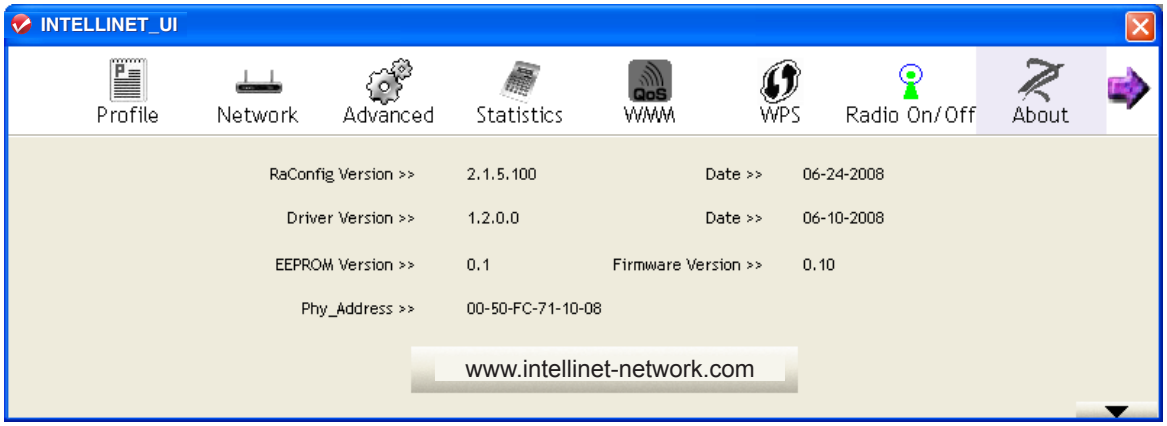


3.8 About

The "About" screen lists version numbers and other information about the card.

1. From whichever section you're currently viewing in the utility, you'll see the About icon in the menu bar of the screen. Otherwise, right-click the configuration utility icon and click "Launch Config Utility."

2. Click "About" to view the card information.

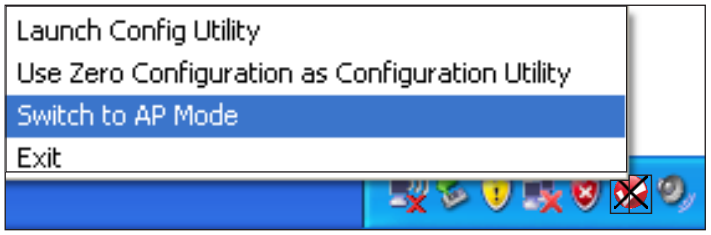


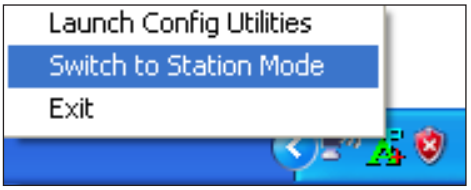
4 SoftAP

In addition to serving as a wireless client of other wireless access points, the Wireless 150N PCI Card can act as a wireless service provider. By switching the card's operating mode to AP, other computers and wireless devices can connect to your computer wirelessly and even share the Internet connection you have.

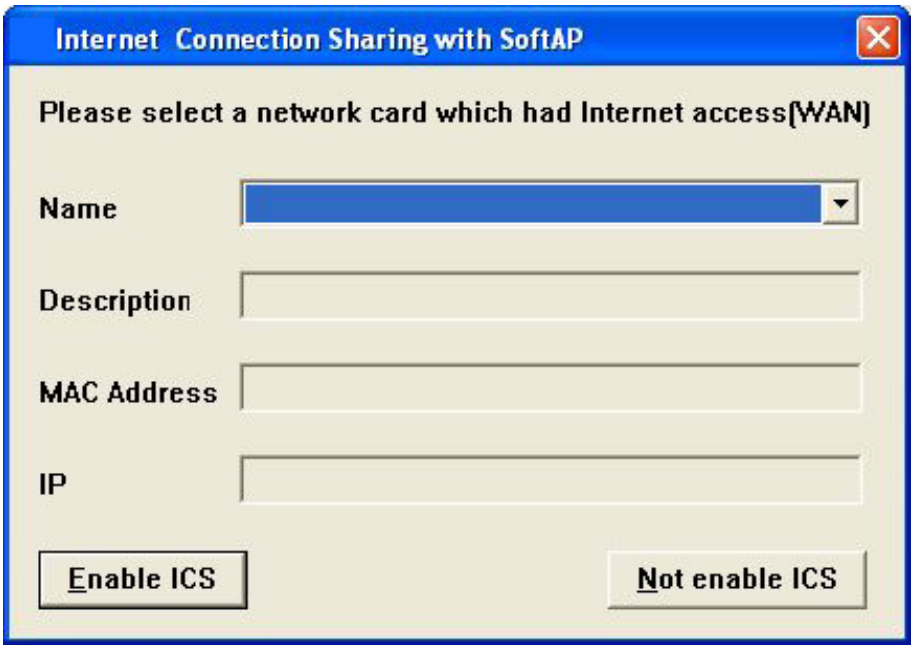
4.1 SoftAP Configuration

By default, the operating mode of the Wireless 150N PCI Card is Station mode (acting as a client of other wireless access points). To switch to AP mode, right-click the configuration utility icon and click "Switch to AP Mode." The utility icon will change to an AP icon (right) to indicate that the card is now operating in AP mode. To switch the wireless card back to Station mode (act as a client of other wireless access points), click "Switch to Station Mode."

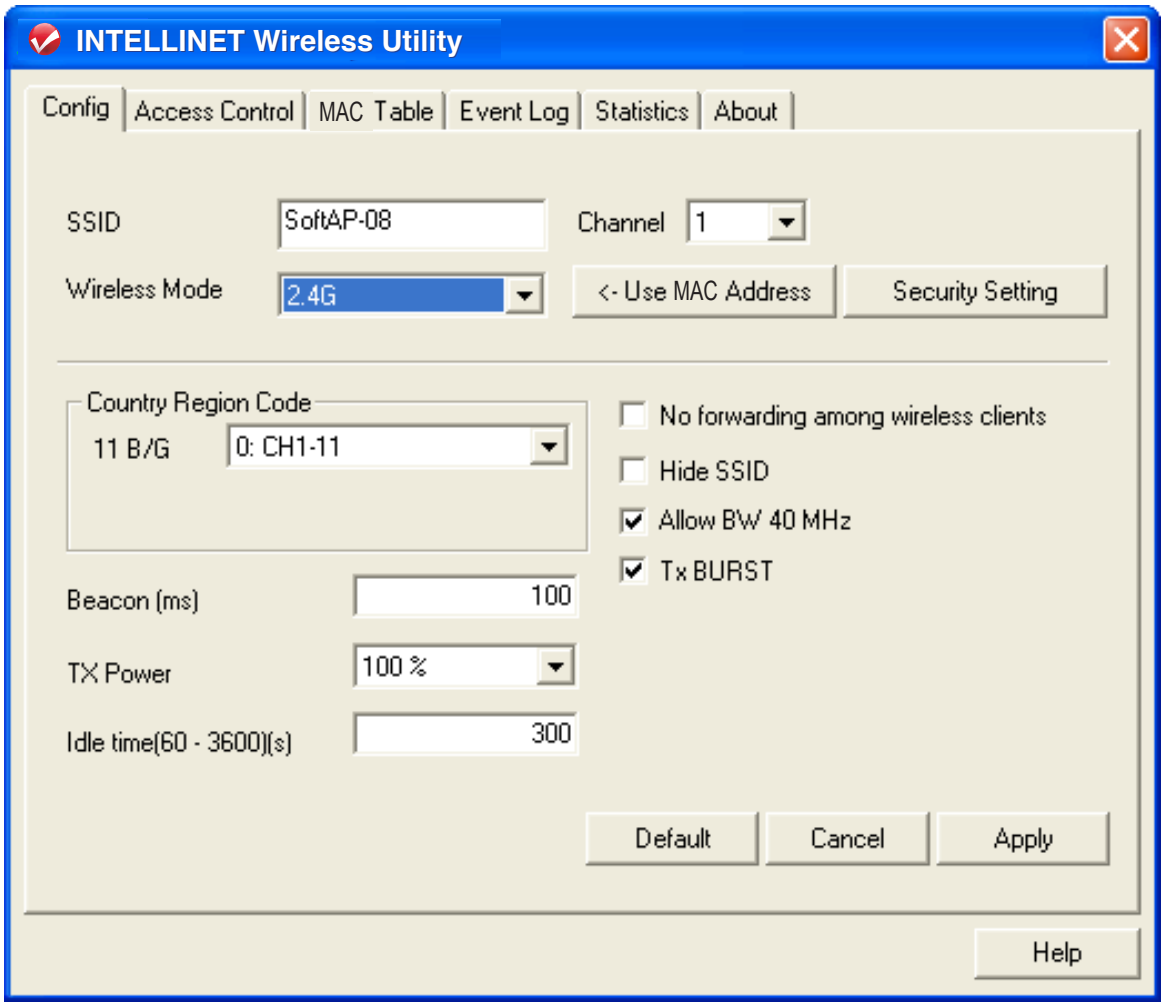




After you switch the operation mode to AP, a configuration window will display, prompting you to assign an existing network card with Internet connection.



If your computer has another network card connected to the Internet, select it from the “Name” drop-down menu and click “Enable ICS.” If your computer *doesn’t* have another network card with Internet connection, click “Not enable ICS.” The Config (Basic Configuration) screen for the AP function will display, providing you with labeled tabs for access to the five other primary menu options (in addition to sub-menus such as Use MAC Address and Security Setting, as detailed below).



SSID — Enter the SSID (the name used to identify this wireless access point) using up to 32 numerical characters and spaces.

Channel — Select the wireless channel you want to use. The number of channels available here depends on the setting of “Country Region Code.”

Wireless Mode — Select the operation mode of the access point.

Use Mac Address — Click to use the MAC address of the card as the SSID. An “AP” prefix will be added automatically.

Security Setting — Set the security options (wireless data encryption). Refer to Section 4.2: Security Settings for details.

Country Region Code — Select the country code of the country or region you're in. Options are 0-7, which will affect the available wireless channels you can use:
0: FCC (U.S., Canada and other countries using FCC radio communication standards)
1: ETSI (Europe)
2: Spain
3: France
4: MKK
5: MKKI (TELEC)
6: Israel (channels 3 to 9)
7: Israel (channels 5 to 13)

No forwarding among wireless clients — When selected, wireless clients won't be able to share data with each other.

Hide SSID — When selected, the SSID will not be broadcast to the public. Your wireless clients must know the exact SSID to be able to connect to your computer. This option is useful to enhance the level of security.

Allow BW 40 MHz — Select to allow BW 40 MHz capability.

Tx Burst — Select to accelerate the data transmit rate. ***NOTE:*** It may not work with all wireless access points and wireless devices.

Beacon (ms) — You can define the time interval that a beacon signal should be sent. The default value is 100. ***NOTE:*** Do not modify this value unless you know what will be affected.

Tx Power — Select a proper output power setting according to your actual needs. For example, you may not need 100% of output power if other wireless clients are not far from you.

Idle Time — Select the idle time for the wireless access point.The default value is 300. ***NOTE:*** Do not modify this value unless you know what will be affected.

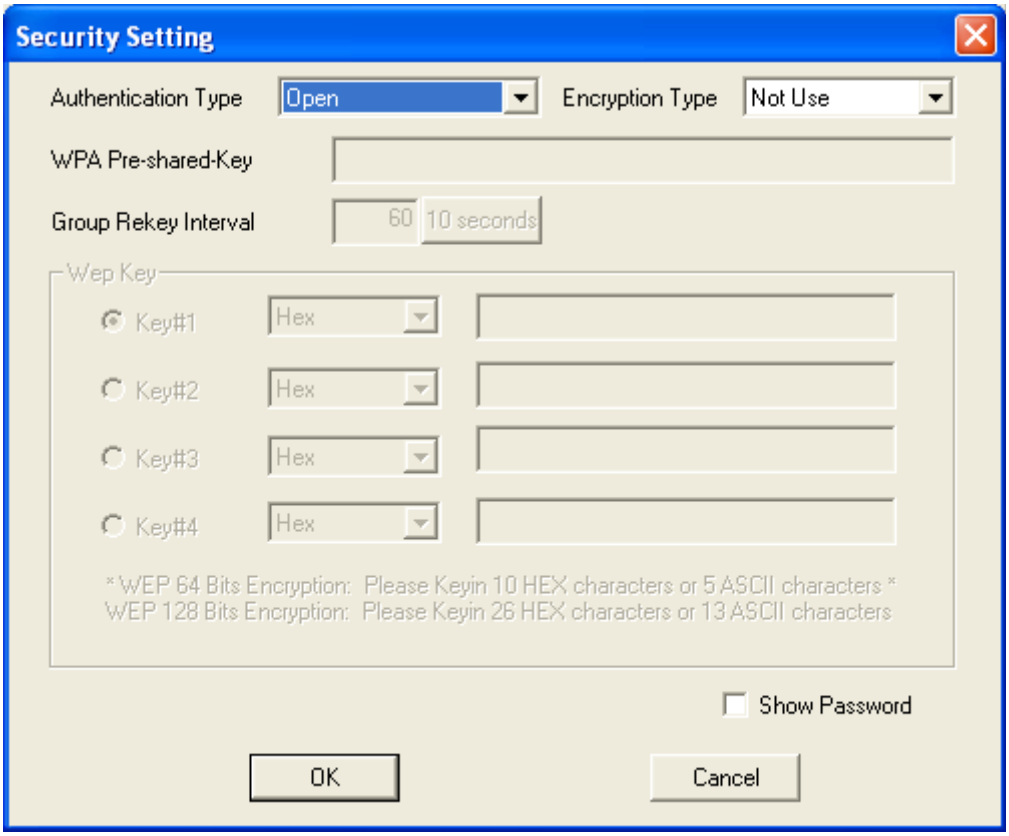
To save changes, click "Apply." Click "Default" to reset all values to factory defaults.

4.2 Security Settings

This Wireless 150N PCI Card supports wireless encryption in AP mode, which will encrypt the data being transferred over the air to enhance the data security level. It's recommended that you enable data encryption unless you want to open your computer (and its Internet connection) to the public. Click "Security Setting" on the Config screen to display the options below.

Authentication Type — Select from among the available options: "Open," "Shared," "WPA-PSK," "WPA2-PSK" and "WPA-PSK / WPA2-PSK." To disable wireless data encryption, select "Open."

Encryption Type — Select from among the available options, which will vary



depending on the authentication type you select. If you select “Not Use,” data will not be encrypted and people with some networking knowledge and the proper tools will be able to read the data you transfer.

WPA Pre-shared Key — Only clients with the same pre-shared key you enter here will be able to connect to your computer. This setting is only available when you select one of the WPA encryptions.

Group Rekey Interval — Specify the time interval to re-issue the key to your wireless clients here. Click “10 seconds” (every 10 seconds) or “Kpackets” (a thousand data packets times the value specified in the “Group Rekey Interval” field).

WEP Key — If you selected WEP as the encryption type, enter the WEP encryption key here. There are two types of WEP key: hex (numbers 0 to 9 and ASCII characters A to F); and ASCII (all alphanumerical characters plus symbols). Select the type of WEP key first, then enter the WEP key according to the type of WEP key you selected.

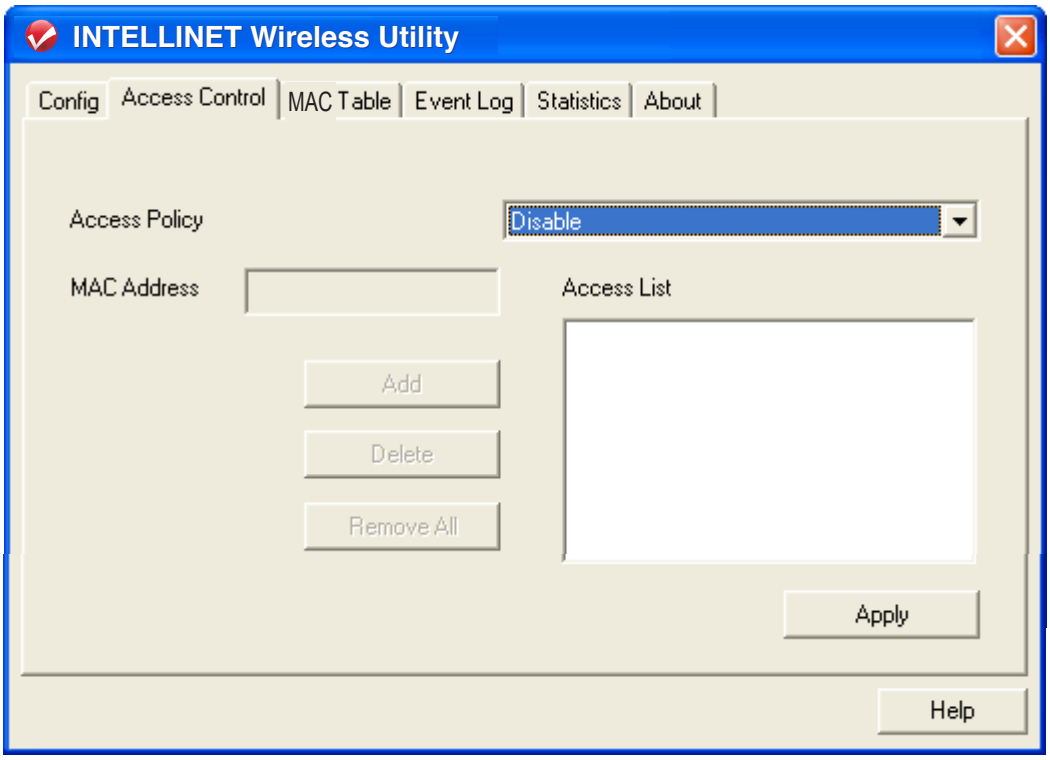
- To use WEP 64-bit encryption, enter 10 characters if you select “Hex” or five characters if you select “ASCII.”
- To use WEP 128-bit encryption, enter 26 characters if you select “Hex” or 13 characters if you select “ASCII.” ***NOTE:*** 128-bit encryption is safer than 64-bit, but the data transfer speed will be slightly reduced.

Show Password — When selected, the key you entered will be shown.

To save changes, click “OK”; click “Cancel” to discard the changes.

4.3 Access Control

If you’re not going to open your computer and wireless resources to the public, you can usethe MAC address filtering function to enforce your access control policy so only wireless clients with the MAC address you define using this function can be connected to your software access point (SoftAP).



Access Policy — Select the policy type of your access rule.

- Disable: Allow any wireless client with proper authentication settings to connect to this access point.
- Allow All: Only allow wireless clients with MAC address listed here to connect to this access point.
- Reject All: Prevent wireless clients with MAC addresses listed here from connecting to this access point.

MAC Address — Enter the MAC address of the wireless client you want to allow or reject. No colon (:) or hyphen (-) required.

Add — Add the MAC address you entered in the “MAC Address” field to the list.

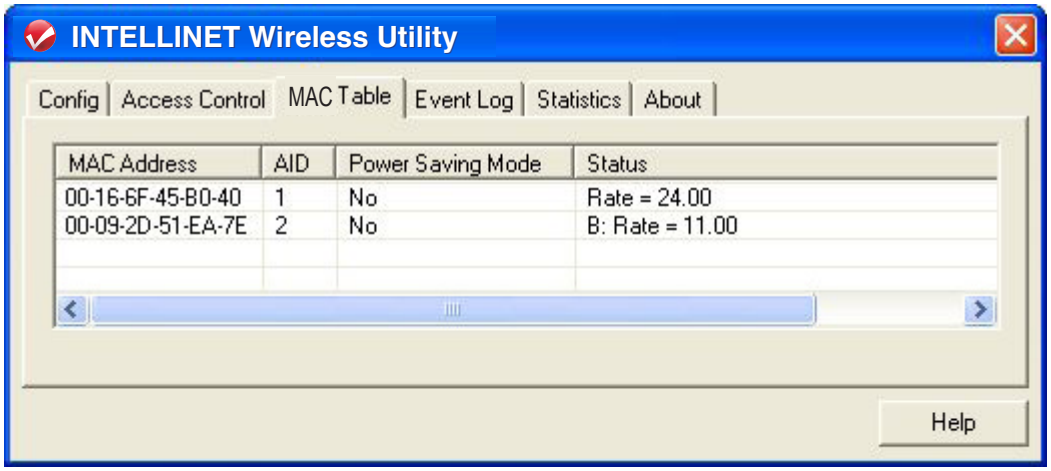
Delete — Select a MAC address from the list, then click “Delete.”

Remove All — Click to delete all MAC addresses in the list.

Click “Apply” to save changes.

4.4 Connection Table

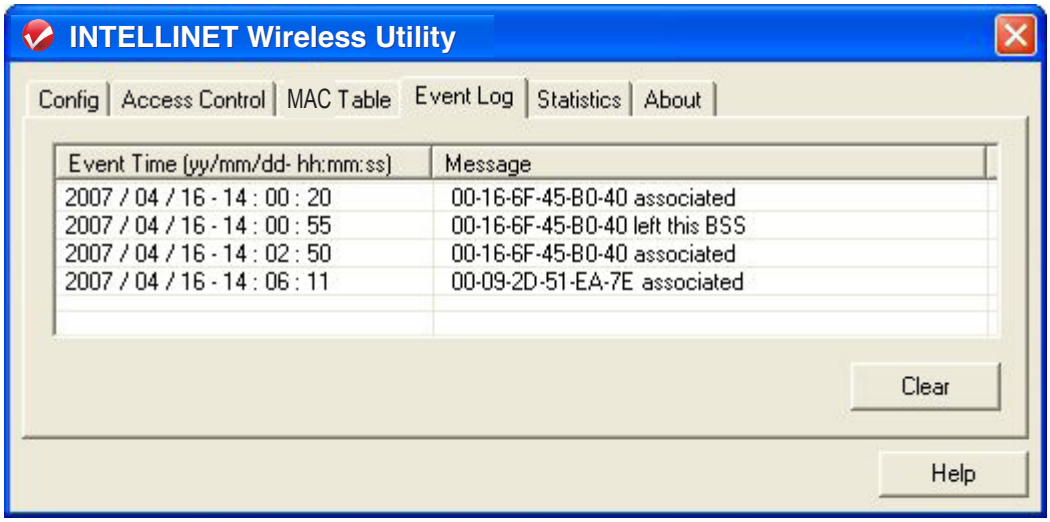
To view a list of all wireless clients connected to this access point, click “MAC Table.”



MAC Address — Displays the MAC address of this wireless client.
AID — This is the serial number of this wireless connection.
Power Saving Mode — Displays the capability of the power-saving function of this wireless client.
Status — Displays additional information about this wireless connection, such as the current wireless operating mode and data transfer rate.

4.5 Event Log

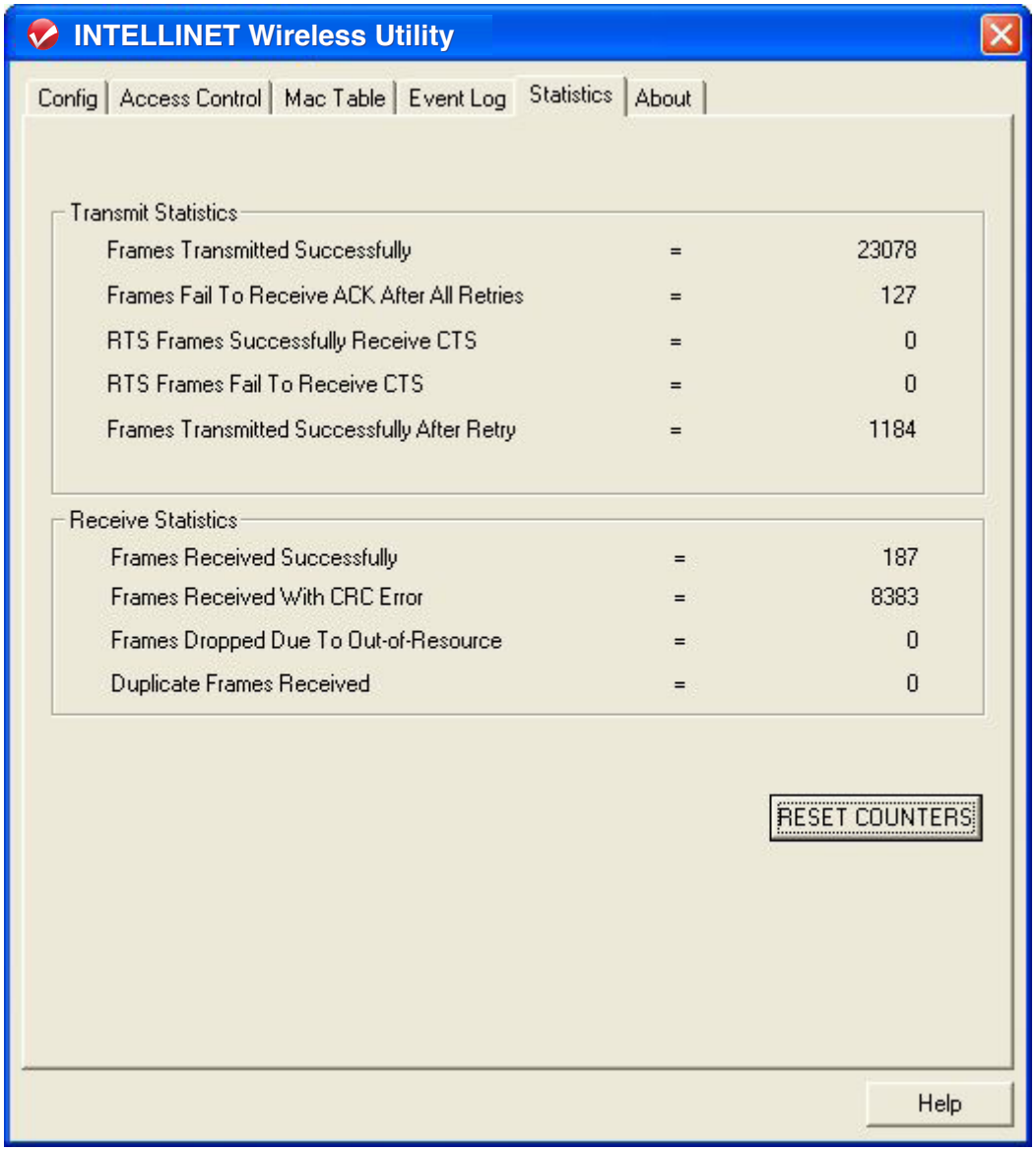
The SoftAP function will log all wireless-related activities as a log. Click “Event Log” to display it.



Clear — Click to remove all entries in the log.

4.6 Statistics

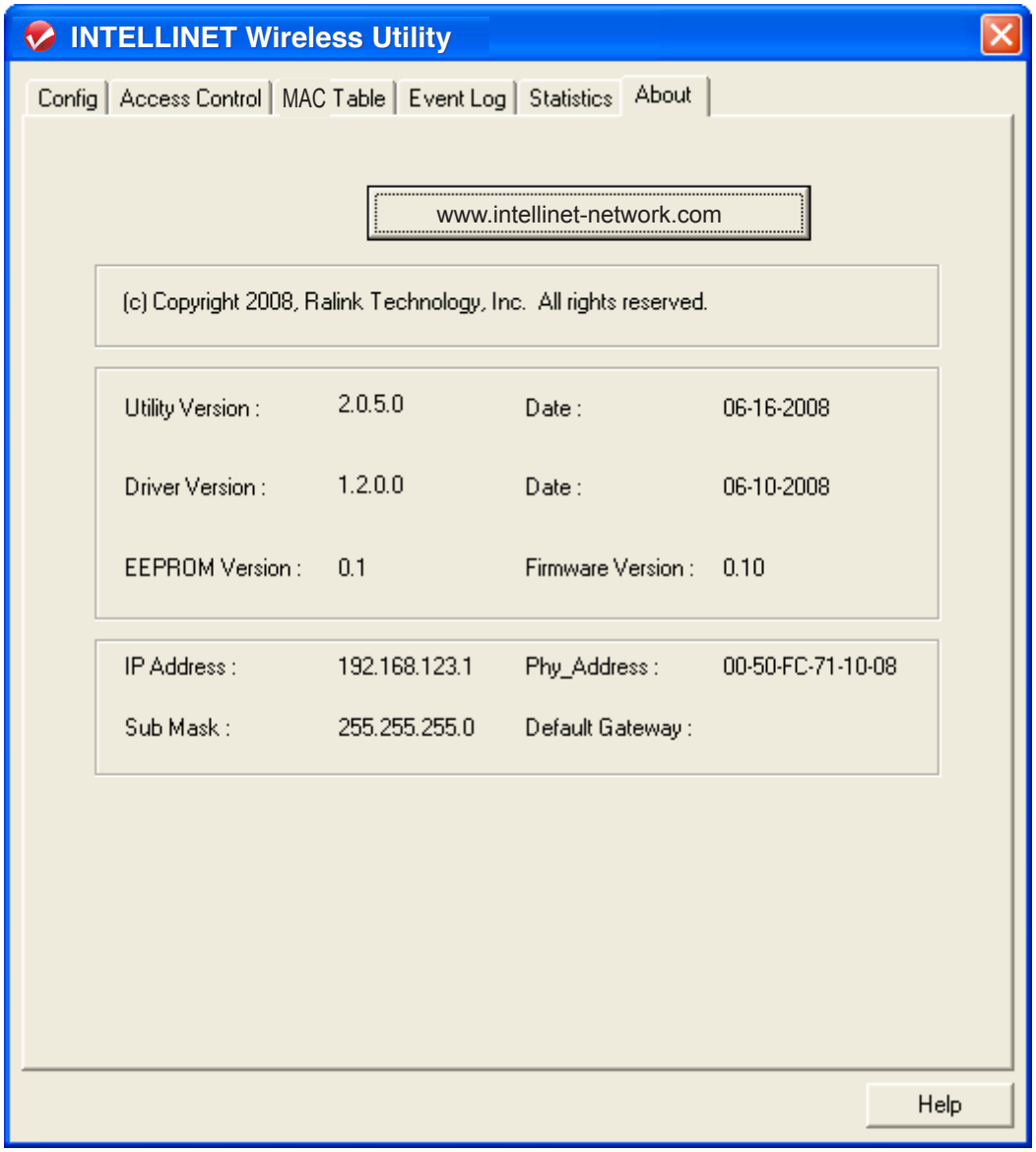
To view detailed information about how your software access point works, click “Statistics” to display the event log.


INTELLINET Wireless Utility
Config
Access Control
Mac Table
Event Log
Statistics
About
Transmit Statistics
Frames Transmitted Successfully = 23078
Frames Fail To Receive ACK After All Retries = 127
RTS Frames Successfully Receive CTS = 0
RTS Frames Fail To Receive CTS = 0
Frames Transmitted Successfully After Retry = 1184
Receive Statistics
Frames Received Successfully = 187
Frames Received With CRC Error = 8383
Frames Dropped Due To Out-of-Resource = 0
Duplicate Frames Received = 0
RESET COUNTERS
Help

Reset Counters — Click to reset all counters to zero.

4.7 About

The “About” screen lists version numbers and other information about the card.



5 TROUBLESHOOTING

If you encounter any problems when you're using the Wireless 150N PCI Card, don't panic! Before you call your place of purchase for help, check this troubleshooting table: The solution to your problem could be very simple, allowing you to solve the problem yourself!

Problem: Can't find any wireless access point / wireless device in the Site Survey section.

Possible Solutions:

1. Click "Rescan" a few more times to see if you can find any wireless access points or wireless devices.
2. Move closer to any known wireless access point.
3. Make sure the Ad Hoc mode is enabled for the wireless device you want to establish a direct wireless link to.
4. Adjust the position of the antenna and click "Rescan" a few more times.

Problem: Nothing happens when "Launch Config Utilities" is clicked.

Possible Solutions:

1. Make sure the card is firmly inserted into your computer's PCI slot. If the configuration utility's icon is black, the ard isn't detected by your computer. Switch the computer off and insert the card again.
2. Reboot the computer and try again.
3. Remove the driver and re-install.
4. Contact your place of purchase for help.

Problem: Can't establish a connection with a certain wireless AP.

Possible Solutions:

1. Click "Connect" a few more times.
2. If the SSID of the access point you want to connect to is hidden (nothing is displayed in the "SSID" field in the Site Survey section), you need to input the correct SSID of the access point. Contact the owner of access point to obtain the correct SSID.
3. You need to enter the correct passphrase / security key to connect to an access point with encryption. Contact the owner of access point to obtain the correct passphrase / security key.
4. The access point you want to connect to only allows network cards with specific MAC address to establish a connection. Go to the About screen and write down the value of "Phy_Addess," then present this value to the owner of the access point so they can add the MAC address of your card to their access point's list.

Problem: The network is slow — difficulty when transferring large files.

Possible Solutions:

1. Move closer to the access point.
2. Enable “Wireless Protection” in the Advanced section.
3. Disable “Tx Burst” in the Advanced section.
4. Enable “WMM” in the WMM section if you need to use multimedia/telephony-related applications.
5. Disable “WMM–Power Save Enable” in the WMM section.
6. There could be too many people using the same radio channel. Ask the owner of the access point to change the channel number.

6 FREQUENTLY ASKED QUESTIONS

Some common questions about references in this user manual are answered below.

What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

- A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b, including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.
- A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

What is the IEEE 802.11b standard?

It’s the IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufacturers to communicate.

What does IEEE 802.11 feature support?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

What is Ad Hoc?
An Ad Hoc integrated wireless LAN is a group of computers, each with a wireless LAN card. Connected as an independent wireless LAN, it's applicable at a departmental scale for a branch or SOHO operation.

What is Infrastructure?
An integrated wireless and wired LAN is called an Infrastructure configuration. It's applicable to enterprise scale for wireless access to a central database or wireless application for mobile workers.

What is BSS ID?
A specific Ad Hoc LAN is called a basic service set (BSS). Computers in a BSS must be configured with the same BSS ID.

What is WEP?
WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802 .11 standard.

Can information be intercepted while transmitting over the air?
WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

What is DSSS? What is FHSS? And what are their differences?
Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband

noise and is rejected (ignored) by most narrowband receivers.

What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

What is WMM?

Wi-Fi Multimedia (WMM) is a group of features for wireless networks that improves the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority.

What is WMM Power Save?

WMM Power Save is a set of features for Wi-Fi networks that increase the efficiency and flexibility of data transmission in order to conserve power. WMM Power Save has been optimized for mobile devices running latency-sensitive applications such as voice, audio or video, but can benefit any Wi-Fi device. WMM Power Save uses mechanisms included in the IEEE 802.11e standard and is an enhancement of IEEE 802.11 legacy power save. With WMM Power Save, the same amount of data can be transmitted in a shorter time while allowing the Wi-Fi device to remain longer in a low-power “dozing” state.

What is WPS?

WPS stands for Wi-Fi Protected Setup. It provides a simple way to establish unencrypted or encrypted connections between wireless clients and access points automatically. A user can press a software or hardware button to activate the WPS function, and WPS-compatible wireless clients and access points will establish connection by themselves. There are two types of WPS: PBC (Push-Button Configuration) and PIN code.

7 SPECIFICATIONS

Standards

- IEEE 802.11b (11 Mbps Wireless LAN)
- IEEE 802.11g (54 Mbps Wireless LAN)
- IEEE 802.11n (150 Mbps Wireless LAN)
- IEEE 802.11e (Wireless Multimedia Extensions (WME))

General

- Bus type: 32-bit PCI card
- Chipset: Ralink RT3060
- Frequency band: 2.4000 – 2.4835 GHz (Industrial Scientific Medical Band)
- Modulation technologies:
  - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
  - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
  - 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Security:
  - 64/128-bit WEP data encryption
  - WPA and WPA2
  - Cisco CCX
- Transmit power:
  - 150 Mbps OFDM, 15 dBm +/- 1.5 dBm
  - 54 Mbps OFDM, 15 dBm +/- 1.5 dBm
  - 11 Mbps CCK, 17 dBm +/- 1.5 dBm
- Receive sensitivity:
  - 150 Mbps OFDM: -68 dBm +/- 1.5 dBm
  - 54 Mbps OFDM: -72 dBm +/- 1.5 dBm
  - 11 Mbps CCK: -90 dBm +/- 1.5 dBm
- Antenna: detachable dipole antenna with RP-SMA connector and 3 dBi gain
- Certification: FCC Class B, CE

Environmental

- Dimensions: 22 (H) x 128 (W) x 121 (L) mm (0.9 x 5.0 x 4.8 in.)
- Weight: 0.275 kg (0.6 lbs.)
- Operating temperature: 0 – 55°C (32 – 131°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -20 – 65°C (4 – 149°F)

System Requirements

- Desktop PC with Pentium 300 MHz-compatible processor or higher
- Windows 2000/XP/2003/Vista and Windows 7
- Available 32-bit PCI slot

Package Contents

- Wireless 150N PCI Card
- 1 antenna
- Quick install guide
- Setup CD with user manual

INTELLINET NETWORK SOLUTIONS™ offers a complete line
of active and passive networking products.
Ask your local computer dealer for more information or visit
www.intellinet-network.com.

Copyright © INTELLINET NETWORK SOLUTIONS
All products mentioned are trademarks or registered trademarks of their respective owners.